JAKSA
JURNAL KAJIAN ILMU HUKUM DAN POLITIK

LPPM Universitas Sains dan Teknologi Komputer
Vol. 4 No. 1 Januari 2026, Hal. 79-94
E-ISSN: 2988-5140; P-ISSN: 2988-7747
Link: https://journal.stekom.ac.id/index.php/Jaksa/index

Implementasi Prinsip *Due Diligence* dalam Kewajiban Negara Mencegah *Cyber* Attacks: Tinjauan Hukum Internasional Kontemporer

Berliant Pratiwi*[1], Neilin Nikhlis[2]
[1]*Program Studi Hukum, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia*
[2]*Program Studi Sitem Komputer, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia*
E-mail: berliant@stekom.ac.id[*1], *neilin@stekom.ac.id*[2]

Article Info

Keywords:
Due diligence, State Responsibility, Cyber Governance, International Law, Indonesia.

Abstract

The rapid evolution of cyberspace has transformed it into a strategic domain of international relations, raising complex legal challenges regarding state responsibility for preventing cross-border cyberattacks. This study explores the implementation of the due diligence principle in international law as a normative foundation for evaluating a state's obligation to prevent harmful cyber activities originating from its territory. Utilizing a normative-legal approach, the research analyzes global legal instruments, state practices, and Indonesia's position on due diligence. Findings reveal a significant gap between the doctrinal recognition of due diligence and its operational application, especially in developing countries lacking institutional and regulatory capacity. The study proposes practical recommendations for integrating due diligence into national Cybersecurity strategies while contributing to the broader development of binding international cyber norms. By focusing on Indonesia, the research aims to strengthen both national legal preparedness and its international legal standing in cyberspace governance.

DOI: ***https://doi.org/10.51903/172frz12***
Submitted: 08 June 2025, Revised: 30 Oct 2025, Accepted: 24 Dec 2025
**Corresponding Author*

Abstrak

Perkembangan pesat ruang siber telah mengubahnya menjadi domain strategis dalam hubungan internasional, yang memunculkan tantangan hukum kompleks terkait tanggung jawab negara dalam mencegah serangan siber lintas batas. Penelitian ini mengkaji penerapan prinsip *due diligence* dalam hukum internasional sebagai landasan normatif untuk menilai kewajiban negara dalam mencegah aktivitas siber berbahaya yang berasal dari wilayahnya. Dengan menggunakan pendekatan yuridis-normatif, penelitian ini menganalisis instrumen hukum global, praktik negara, serta posisi Indonesia terhadap prinsip *due diligence*. Hasil penelitian menunjukkan adanya kesenjangan yang signifikan antara pengakuan doktrinal terhadap prinsip ini dengan penerapan operasionalnya, terutama di negara berkembang yang memiliki kapasitas kelembagaan dan regulasi terbatas. Studi ini juga memberikan rekomendasi praktis untuk mengintegrasikan prinsip *due diligence* ke dalam strategi keamanan siber nasional, sekaligus berkontribusi pada pengembangan norma hukum siber internasional yang mengikat. Dengan menjadikan Indonesia sebagai fokus kajian, penelitian ini bertujuan memperkuat kesiapan hukum nasional dan posisi hukum internasional Indonesia dalam tata kelola ruang siber global.

Kata Kunci: *Due diligence, Tanggung Jawab Negara, Tata Kelola Siber, Hukum Internasional, Indonesia*

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang begitu cepat dalam dua dekade terakhir telah mengubah hampir semua aspek kehidupan modern, termasuk cara negara-negara menjalankan

pemerintahan dan menjaga keamanan nasionalnya (Lehto, 2022). Dunia maya atau ruang siber kini menjadi arena baru bagi interaksi antarnegara, baik dalam bentuk kerja sama maupun konfrontasi (Schmitt, 2023). Sayangnya, seiring dengan meningkatnya ketergantungan negara terhadap infrastruktur digital, muncul pula ancaman-ancaman baru, salah satunya adalah serangan siber (Cinini et al., 2023). Fenomena ini telah menjelma menjadi isu global karena sifat serangannya yang tidak mengenal batas wilayah dan dapat dilakukan secara tersembunyi dari belahan dunia mana pun (Yaacoub et al., 2022).

Serangan siber bukan hanya mengancam sistem teknologi suatu negara, tetapi juga berpotensi melemahkan kepercayaan publik, mengganggu kestabilan ekonomi, dan bahkan memicu konflik antarnegara (Egloff & Smeets, 2023). Dalam konteks ini, muncul pertanyaan penting: sejauh mana negara bertanggung jawab untuk mencegah aktivitas siber berbahaya yang berasal dari wilayahnya (Guo et al., 2023).Di sinilah prinsip *due diligence* dalam hukum internasional menjadi relevan. Prinsip ini menegaskan bahwa negara memiliki kewajiban untuk memastikan bahwa wilayah atau sistem di bawah yurisdiksinya tidak digunakan sebagai basis untuk merugikan negara lain—baik oleh individu, kelompok, maupun entitas lain (Islam et al., 2025).

Situasi global menunjukkan bahwa serangan siber lintas negara mengalami peningkatan yang signifikan (Nowak & Distel, 2024). Laporan (Staves et al., 2022) mencatat adanya lebih dari 80 insiden besar serangan siber yang melibatkan aktor negara, termasuk kasus pencurian data besar-besaran dari sistem pemerintah Amerika Serikat dan gangguan terhadap infrastruktur energi Ukraina. Meski sulit dibuktikan keterlibatan langsung pemerintah dalam kasus-kasus tersebut, banyak dari aktivitas tersebut diketahui berasal dari wilayah negara tertentu tanpa adanya tindakan pencegahan yang memadai dari negara asal (Shandler & Gomez, 2023). Kondisi ini memperkuat urgensi untuk mengkaji kewajiban negara dalam konteks hukum internasional, terutama mengenai pencegahan serangan siber yang bersumber dari dalam yurisdiksinya (Ukwandu et al., 2022).

Di Indonesia sendiri, situasinya juga memprihatinkan. Badan Siber dan Sandi Negara (BSSN) mencatat adanya lebih dari 1,6 miliar anomali trafik siber sepanjang tahun 2023 (Fajri & Harwahyu, 2024). Serangan ini tidak hanya menyasar sektor pemerintahan, tetapi juga sektor-sektor penting seperti keuangan, kesehatan, dan pendidikan (Imoize et al., 2023). Ancaman ini memperlihatkan bahwa tanpa sistem pengawasan dan pencegahan yang baik, wilayah suatu negara bisa dengan mudah dijadikan “markas” oleh pelaku kejahatan siber internasional (Alramamneh & Abuanzeh, 2023). Jika negara tidak mampu atau tidak mau mengambil tindakan untuk mencegah hal tersebut, maka secara normatif negara bisa dinilai melanggar kewajiban hukumnya menurut prinsip *due diligence* (Asmare & Ayalew, 2023).

Dalam literatur hukum internasional, prinsip *due diligence* bukanlah hal yang baru. Prinsip ini sudah lama dikenal, terutama dalam kasus-kasus terkait perlindungan lingkungan dan pencegahan kejahatan lintas batas (Wilhelm, 2024). (Gustafsson et al., 2023) dalam tulisannya menjelaskan bahwa negara

wajib mengambil langkah-langkah wajar untuk mencegah kerugian terhadap negara lain, bahkan jika kerugian itu disebabkan oleh pihak non-negara. Dalam konteks dunia maya, prinsip ini kemudian diadopsi dalam dokumen (Schilling-Vacaflor & Gustafsson, 2024), yang menjadi salah satu referensi penting dalam pengembangan hukum siber internasional. Dokumen tersebut menekankan bahwa meskipun tidak ada kewajiban absolut untuk mencegah semua serangan, negara harus mampu menunjukkan bahwa telah melakukan langkah yang wajar untuk mencegah penggunaan sistemnya oleh pihak yang berniat merusak (Schilling-Vacaflor & Lenschow, 2023).

Meski demikian, tantangan utama yang muncul adalah belum adanya standar internasional yang jelas mengenai sejauh mana prinsip *due diligence* ini berlaku di dunia maya (Moynihan, 2023). (Bannelier, 2024) mengemukakan bahwa sifat dunia digital yang anonim dan lintas batas membuat banyak norma hukum tradisional sulit diterapkan. Negara sering kali tidak memiliki alat atau kapasitas untuk mengawasi aktivitas digital di dalam wilayahnya secara penuh. Selain itu, ketidaksepakatan di antara negara-negara besar mengenai batas-batas kewajiban hukum dalam ranah siber semakin memperumit implementasi prinsip ini (Katagiri, 2024).

Beberapa peneliti bahkan menilai bahwa prinsip *due diligence* masih belum benar-benar mendapat tempat dalam kebijakan siber nasional di banyak negara. (Sachoulidou, 2023) mencatat bahwa ada kecenderungan negara-negara untuk menunda adopsi prinsip ini karena khawatir akan menambah beban hukum dan teknis bagi mereka. Di sisi lain, dalam konteks Indonesia, kajian hukum mengenai tanggung jawab negara terhadap aktivitas siber masih belum berkembang secara signifikan (Sankaran & Church, 2023). Literatur hukum lebih banyak membahas aspek teknis seperti keamanan siber dan perlindungan data pribadi, sementara aspek normatif tentang tanggung jawab negara secara internasional, termasuk penerapan prinsip *due diligence*, masih jarang dibahas secara mendalam (Żuk & Żuk, 2024).

Penelitian sebelumnya juga banyak terfokus pada kebijakan keamanan nasional tanpa mengaitkannya secara eksplisit dengan kewajiban internasional. Padahal, dalam konteks global saat ini, di mana interaksi antarnegara di dunia maya semakin kompleks, penting bagi suatu negara untuk memahami peran dan tanggung jawab hukumnya di mata dunia. Sebagai negara yang mulai aktif dalam forum-forum tata kelola internet global seperti IGF (Internet Governance Forum) dan pembahasan norma siber di PBB, Indonesia perlu menunjukkan komitmen terhadap prinsip-prinsip internasional, termasuk *due diligence*.

Studi lain yang dilakukan oleh (Agir et al., 2023) menunjukkan bahwa keberhasilan implementasi *due diligence* sangat bergantung pada kapasitas suatu negara—baik dari sisi teknis, hukum, maupun institusional. Negara-negara yang memiliki kerangka hukum yang kuat serta lembaga yang berfungsi secara efektif dalam pemantauan dan pencegahan aktivitas siber cenderung lebih mampu melaksanakan kewajiban ini (Malhotra et al., 2022). Sementara itu, negara berkembang seperti Indonesia menghadapi tantangan ganda: di satu sisi harus membangun infrastruktur siber yang

tangguh, di sisi lain dituntut untuk mengikuti standar hukum internasional yang sedang berkembang (Wang et al., 2023).

Dari sini terlihat jelas adanya kesenjangan atau gap yang cukup signifikan. Pertama, belum ada kejelasan normatif di tingkat global mengenai implementasi prinsip *due diligence* dalam domain siber. Meskipun secara prinsipil negara diwajibkan untuk mencegah aktivitas berbahaya, tidak ada satu instrumen hukum internasional yang secara tegas mengatur langkah-langkah apa yang harus dilakukan negara. Kedua, di tingkat nasional, Indonesia belum memiliki instrumen hukum yang secara eksplisit mengadopsi prinsip ini dalam kebijakan siber nasionalnya. Hal ini membuat Indonesia rentan terhadap kritik internasional bila dianggap lalai dalam mengontrol aktivitas siber dari wilayahnya.

Penelitian ini hadir untuk menjawab kesenjangan tersebut. Tujuan utama dari penelitian ini adalah untuk mengkaji secara mendalam bagaimana prinsip *due diligence* dapat diimplementasikan oleh negara, khususnya Indonesia, dalam mencegah aktivitas siber lintas batas yang membahayakan negara lain. Penelitian ini mengombinasikan pendekatan normatif dengan analisis terhadap praktik yang berkembang di tingkat global, sekaligus menelaah bagaimana posisi Indonesia dalam kerangka hukum internasional tersebut.

Penelitian ini berkontribusi dengan merumuskan model hukum nasional yang mampu mengakomodasi kewajiban negara untuk mencegah aktivitas siber berbahaya melalui penerapan prinsip *due diligence*, sebagai bagian dari kewajiban hukum internasional modern. Model konseptual yang ditawarkan memberikan dasar normatif yang lebih kuat bagi Indonesia dalam membangun kerangka hukum keamanan siber yang responsif, sejalan dengan perkembangan hukum internasional kontemporer.

II. METODOLOGI PENELITIAN

A. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan normatif-yuridis yang bertumpu pada analisis terhadap norma-norma hukum internasional yang berlaku, termasuk prinsip-prinsip kebiasaan internasional, traktat, serta doktrin dan yurisprudensi yang relevan. Pendekatan ini dipilih karena fokus utama penelitian adalah menelaah kewajiban negara dalam mencegah serangan siber melalui implementasi prinsip *due diligence*, yang merupakan bagian dari hukum internasional publik. Selain itu, pendekatan ini memungkinkan telaah mendalam terhadap kerangka hukum yang sudah ada, termasuk kekosongan norma atau ketidakkonsistenan dalam penerapannya di konteks dunia maya. Untuk memperjelas proses penelitian ini, gambar 1 menunjukkan kerangka konseptual yang menggambarkan alur pendekatan normatif-yuridis yang digunakan.

Gambar 1. Kerangka Konseptual Metode Penelitian

Pendekatan normatif diperkuat dengan analisis konseptual, untuk memahami perkembangan doktrin *due diligence* dalam kerangka hukum internasional kontemporer, serta analisis preskriptif guna merumuskan rekomendasi normatif bagi negara, khususnya Indonesia, agar dapat memenuhi kewajiban hukumnya dalam konteks pencegahan serangan siber. Penelitian ini juga memanfaatkan analisis komparatif terbatas, dengan membandingkan kerangka kebijakan dari beberapa negara lain yang telah mengadopsi prinsip *due diligence* dalam kebijakan sibernya.

B. Jenis dan Sumber Data

Data utama dalam penelitian ini berupa data sekunder yang terdiri dari dokumen hukum internasional, seperti piagam PBB, konvensi-konvensi internasional yang relevan, putusan pengadilan internasional, serta dokumen non-mengikat (soft law) seperti Tallinn Manual 2.0 on the International Law Applicable to *Cyber* Operations. Selain itu, penelitian juga menggunakan laporan dari organisasi internasional seperti Perserikatan Bangsa-Bangsa, International Law Commission (ILC), dan Center for Strategic and International Studies (CSIS).

Sumber akademik seperti buku, artikel jurnal, dan dokumen konferensi ilmiah juga menjadi bagian penting dalam pengumpulan data. Penelusuran dilakukan melalui database terkemuka seperti Scopus, JSTOR, HeinOnline, dan Google Scholar. Selain sumber internasional, penelitian ini juga mengkaji dokumen hukum nasional Indonesia, seperti peraturan perundang-undangan terkait keamanan siber, strategi nasional keamanan siber (Stranas KS), serta laporan dari Badan Siber dan Sandi Negara (BSSN).

C. Teknik Pengumpulan Data

Data dikumpulkan melalui studi kepustakaan yang sistematis dengan metode snowballing untuk menemukan sumber-sumber relevan yang saling terhubung, terutama dalam menjangkau publikasi

yang membahas aspek teknis maupun normatif dari prinsip *due diligence* dalam domain siber. Selain itu, dilakukan penelusuran terhadap state practice dan opinio juris negara-negara tertentu melalui laporan diplomatik, kebijakan luar negeri, serta pernyataan resmi yang diterbitkan oleh kementerian luar negeri atau lembaga keamanan siber masing-masing negara.

Penelitian juga mengumpulkan dokumen hasil negosiasi internasional seperti laporan dari UN GGE (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) dan OEWG (Open-ended Working Group), yang memuat posisi resmi negara terhadap norma hukum internasional di ranah siber.

D. Teknik Analisis Data

Data dianalisis dengan pendekatan hermeneutika hukum, yaitu menafsirkan teks-teks hukum dengan mempertimbangkan konteks, sejarah, dan tujuan pembentukan norma. Pemilihan pendekatan hermeneutika hukum dalam penelitian ini didasarkan pada karakter hukum internasional yang sebagian besar bersumber dari norma non-kodifikasi, seperti customary international law dan prinsip umum hukum (general principles of law). Berbeda dengan hukum positif yang tertulis secara eksplisit, norma-norma ini menuntut proses penafsiran mendalam terhadap praktik negara dan opinio juris untuk memahami maksud dan cakupan kewajiban hukum yang muncul. Hermeneutika hukum relevan karena memungkinkan peneliti menginterpretasikan teks hukum, dokumen internasional, serta pernyataan negara dengan mempertimbangkan konteks historis, politik, dan teleologis pembentukannya. Pendekatan ini juga sejalan dengan metodologi yang digunakan oleh International Law Commission (ILC) dalam mengidentifikasi dan mengklarifikasi norma kebiasaan internasional.

Analisis dilakukan dalam tiga tahap. Pertama adalah identifikasi norma, yaitu tahap di mana prinsip-prinsip hukum yang berkaitan dengan *due diligence* dipetakan dari berbagai dokumen dan praktik internasional. Kedua adalah interpretasi norma, yaitu menganalisis isi, ruang lingkup, dan batas penerapan prinsip *due diligence* di dunia siber. Ketiga adalah evaluasi normatif, yakni menilai sejauh mana prinsip tersebut dapat dan telah diterapkan dalam konteks praktik negara, termasuk implikasinya terhadap posisi hukum Indonesia.

Analisis dilakukan secara induktif dan deduktif. Secara induktif, peneliti mengkaji kasus-kasus konkret serangan siber lintas batas untuk menilai bagaimana negara meresponsnya berdasarkan prinsip *due diligence*. Secara deduktif, peneliti menelusuri bagaimana prinsip tersebut diformulasikan dalam doktrin hukum internasional, kemudian mengujinya terhadap praktik yang ada.

Untuk mendalami konteks Indonesia, digunakan analisis doktrinal terhadap peraturan perundang-undangan nasional yang relevan dengan kewajiban mencegah aktivitas siber lintas batas. Analisis ini difokuskan pada bagaimana regulasi nasional dapat selaras atau perlu diselaraskan dengan standar hukum internasional.

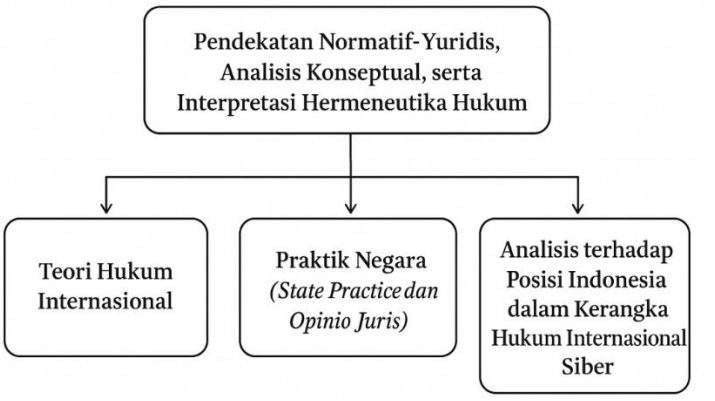
E. Validitas dan Replikasi

Agar hasil penelitian dapat dipertanggungjawabkan dan direplikasi oleh peneliti lain, peneliti menyusun kerangka analisis yang transparan dan sistematis. Setiap sumber hukum yang digunakan dicantumkan dengan kutipan lengkap, dan seluruh langkah analisis dijelaskan secara rinci dalam bagian pembahasan. Peneliti juga mengadopsi prinsip triangulasi sumber, dengan membandingkan data dari berbagai sumber untuk menghindari bias interpretasi. Selain itu, untuk menjaga objektivitas, analisis normatif tidak hanya didasarkan pada doktrin hukum Barat, tetapi juga mempertimbangkan perspektif negara berkembang.

F. Batasan Penelitian

Penelitian ini memiliki batasan pada fokus wilayah, yaitu hanya mengkaji posisi Indonesia dan negara-negara yang telah secara eksplisit menyatakan kebijakan atau kerangka hukum yang berkaitan dengan *due diligence* di dunia siber. Selain itu, karena bersifat normatif, penelitian ini tidak melakukan pengujian teknis atas sistem keamanan siber, melainkan terbatas pada kajian yuridis dan normatif. Namun, batasan ini justru memperkuat fokus penelitian dalam menjawab pertanyaan tentang bagaimana prinsip *due diligence* dapat diterapkan oleh negara dalam rangka memenuhi kewajiban internasionalnya di dunia maya.

Gambar 2 menampilkan alur logis penelitian ini yang mengombinasikan pendekatan normatif-yuridis, analisis konseptual, serta interpretasi hermeneutika hukum. Alur ini menunjukkan hubungan antara teori hukum internasional, praktik negara (state practice dan opinio juris), serta analisis terhadap posisi Indonesia dalam kerangka hukum internasional siber.



Gambar 2. Kerangka Konseptual Metode Penelitian *(Sumber: Disusun oleh penulis (2025) berdasarkan pendekatan normatif-yuridis dan hermeneutika hukum).*

III. HASIL DAN PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa implementasi prinsip *due diligence* dalam konteks hukum internasional masih menghadapi berbagai tantangan, baik di tingkat konseptual maupun praktis. Secara umum, terdapat kesenjangan antara pengakuan prinsip ini dalam doktrin hukum internasional

dengan realitas penerapannya oleh negara-negara. Penelitian ini menemukan bahwa hanya sebagian kecil negara yang secara eksplisit mengadopsi prinsip *due diligence* dalam kebijakan keamanan sibernya. Bahkan, sebagian besar negara berkembang belum memiliki regulasi atau instrumen hukum nasional yang mengatur secara langsung kewajiban negara dalam mencegah aktivitas siber berbahaya dari dalam yurisdiksinya.

Data yang dikumpulkan dari laporan tahunan CSIS menunjukkan peningkatan signifikan jumlah serangan siber lintas negara selama lima tahun terakhir. Jumlah insiden yang dikategorikan sebagai serangan antarnegara meningkat dari 56 kasus pada tahun 2020 menjadi 88 kasus pada tahun 2024. Selain itu, jumlah negara yang terlibat dalam konflik atau tuduhan terkait aktivitas siber juga meningkat, yang mengindikasikan adanya ketegangan geopolitik digital yang semakin tajam. Tabel 1 menunjukkan insiden Siber Global Terbesar (2020–2024). Selain data dalam bentuk tabel, gambar 3 menunjukkan tren peningkatan insiden serangan siber lintas negara pada periode 2020 hingga 2024.

Tabel 1. Insiden Siber Global Terbesar (2020–2024)

Tahun	Jumlah Insiden Global (CSIS)	Jumlah Negara Terlibat
2020	56	14
2021	64	17
2022	72	17
2023	81	23
2024	88	27

Sumber: CSIS (2024), diolah oleh penulis.

Gambar 3. Tren Global Insiden Serangan Siber Lintas Negara (2020–2024)

Penelitian ini juga menganalisis kebijakan dari lima negara representatif: Amerika Serikat, Estonia, Indonesia, Rusia, dan Cina. Dari kelima negara tersebut, hanya Amerika Serikat dan Estonia yang

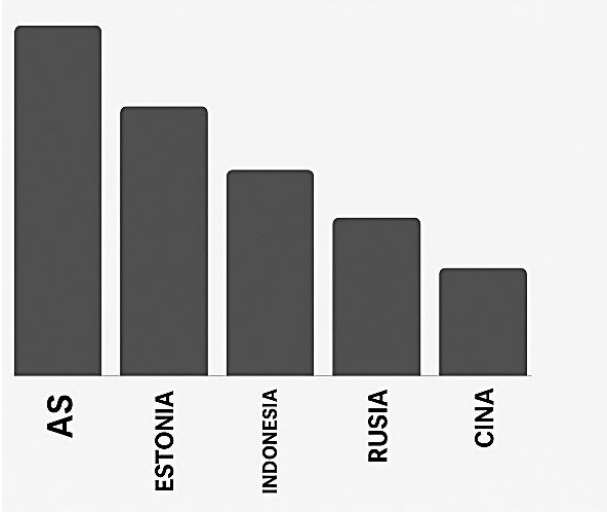
secara eksplisit mengakui prinsip *due diligence* dalam dokumen resmi dan kebijakan nasionalnya. Sementara Indonesia belum memiliki instrumen hukum nasional yang secara khusus mengatur prinsip ini, meskipun terdapat upaya melalui strategi keamanan siber nasional. Rusia dan Cina, meskipun merupakan kekuatan siber global, justru tidak menyatakan dukungan terbuka terhadap prinsip *due diligence* dan lebih mengedepankan prinsip non-intervensi. Untuk lebih jelasnya, tabel 2 menunjukkan respons negara terhadap prinsip *due diligence*.

Tabel 2. Respons Negara terhadap Prinsip *Due diligence*

Negara	Kebijakan Resmi *Due diligence*	Instrumen Tertulis Nasional
AS	Ya	Ada
Estonia	Ya	Tidak Ada
Indonnesia	Tidak	Belum Ada
Rusia	Tidak	Tidak Ada
Cina	Tidak	Tidak Ada

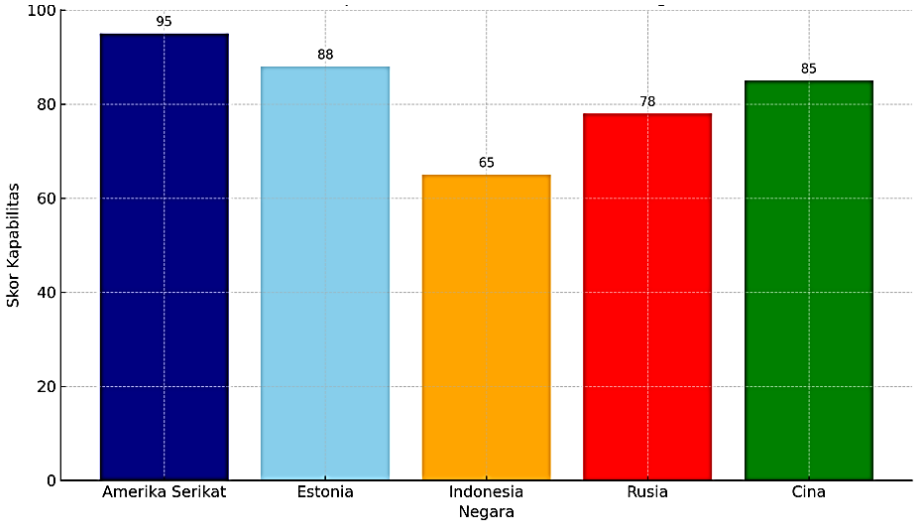
Sumber: UN GGE Reports, National Cyber Strategies (2024), diolah oleh penulis.

Gambar 4 menyajikan perbandingan adopsi prinsip *due diligence* antar negara yang dianalisis.



Gambar 4. Perbandingan Adopsi Prinsip *Due diligence* antar Negara

Untuk memperjelas keterkaitan antara implementasi prinsip *due diligence* dan kapabilitas teknis negara, dilakukan pemetaan kapasitas siber berdasarkan data publik dari indeks global dan strategi nasional. Gambar 5 menyajikan skor kapabilitas lima negara utama yang menjadi objek analisis penelitian ini.



Gambar 5. Skor Kapabilitas lima Negara (*Sumber: Penilaian berdasarkan Global Cybersecurity Index (GCI) dan dokumen strategi siber nasional, diolah oleh penulis).*

Secara khusus, Indonesia masih menghadapi tantangan dalam mengintegrasikan prinsip ini ke dalam kerangka hukum nasional. Tidak adanya aturan eksplisit yang mengatur tanggung jawab negara dalam mencegah aktivitas siber dari wilayahnya menyebabkan lemahnya posisi hukum Indonesia di forum internasional. Hal ini mengindikasikan pentingnya penguatan kapasitas normatif dan kelembagaan guna memenuhi kewajiban internasional secara optimal.

Pembahasan

Temuan penelitian ini memperkuat argumentasi bahwa prinsip *due diligence* merupakan norma penting dalam hukum internasional kontemporer, khususnya dalam domain siber. Prinsip ini tidak hanya bersifat deklaratif, melainkan juga memiliki nilai operasional tinggi dalam mencegah konflik antarnegara. Negara yang melaksanakan prinsip ini secara konsisten dapat memperkuat posisi hukumnya dalam diplomasi siber sekaligus meningkatkan kepercayaan mitra internasional (Bannelier, 2024).

Namun demikian, implementasi prinsip ini masih dihadapkan pada sejumlah kendala serius. Pertama, belum adanya definisi operasional yang disepakati secara internasional mengenai standar minimum tindakan yang harus dilakukan negara mengakibatkan ambiguitas penerapan. Negara-negara pun memiliki interpretasi yang beragam tentang sejauh mana mereka berkewajiban bertindak. Kedua, kapabilitas negara menjadi faktor penting dalam menentukan efektivitas implementasi prinsip ini. Negara maju dengan infrastruktur siber yang kuat lebih mampu memenuhi kewajiban ini dibanding negara berkembang seperti Indonesia (Radanliev, 2024). Ketiga, terdapat ketegangan antara prinsip *due diligence* dan prinsip non-intervention, di mana negara-negara seperti Rusia dan Tiongkok cenderung menolak perluasan prinsip ini karena dianggap membuka peluang intervensi terhadap kedaulatan domestik (Katagiri, 2024).

Sebagaimana ditunjukkan dalam Tabel 2 dan Gambar 4, perbedaan respons negara terhadap prinsip *due diligence* tidak hanya mencerminkan variasi kebijakan, tetapi juga memiliki implikasi langsung terhadap pembentukan customary international law di bidang keamanan siber. Dalam konteks hukum kebiasaan internasional, dua elemen utama yang menentukan lahirnya norma baru adalah state practice (praktik negara yang konsisten) dan opinio juris (keyakinan hukum bahwa praktik tersebut dilakukan karena kewajiban hukum (International Law Commission (ILC), 2022).

Dari sisi state practice, negara-negara seperti Amerika Serikat dan Estonia menunjukkan pola perilaku yang relatif konsisten dalam menerapkan prinsip *due diligence* melalui kebijakan siber nasional dan dokumen resmi seperti *National Cyber Strategy* (United States Government, 2022) dan *Cybersecurity* Act (Government of Estonia, 2023). Praktik berulang ini memperkuat asumsi adanya penerimaan faktual terhadap kewajiban negara untuk mencegah penggunaan infrastruktur sibernya bagi serangan lintas batas. Sebaliknya, sikap Rusia dan Tiongkok yang menolak penerapan prinsip ini atas dasar kedaulatan dan non-intervention justru mencerminkan posisi persistent objector, yaitu negara yang secara konsisten menolak terbentuknya norma kebiasaan internasional baru dalam isu ini. Posisi Indonesia sendiri masih berada di antara dua kutub tersebut: meskipun belum memiliki regulasi eksplisit, pernyataan resmi dalam forum *Open-Ended Working Group* (Open-Ended Working Group, 2023) dan partisipasi aktif dalam *United Nations Group of Governmental Experts* (UN GGE) menunjukkan kecenderungan menuju penerimaan prinsip *due diligence* sebagai kewajiban hukum yang sedang berkembang (*emerging norm*).

Sementara itu, dari sisi opinio juris, terdapat indikasi yang semakin kuat bahwa komunitas internasional mulai memandang *due diligence* sebagai kewajiban hukum yang mengikat secara umum, bukan sekadar pedoman etik. Pernyataan bersama negara-negara Uni Eropa dalam (United Nations Group of Governmental Experts, 2021) serta komentar dari (International Law Commission (ILC), 2022) menegaskan bahwa negara memiliki tanggung jawab hukum untuk mencegah aktivitas siber yang merugikan negara lain, terlepas dari pelaku langsungnya. Walaupun belum mencapai tingkat universalitas penuh, pola ini menunjukkan adanya proses kristalisasi menuju pembentukan norma kebiasaan baru di bidang keamanan siber.

Dengan demikian, perbedaan posisi negara dalam Tabel 2 dan Gambar 4 bukan hanya perbedaan kebijakan administratif, melainkan juga menggambarkan dinamika pembentukan norma kebiasaan internasional (*customary international law*) yang tengah berkembang. Posisi Indonesia yang mulai mengadopsi prinsip ini dalam kebijakan nasional, meski belum secara eksplisit, berpotensi memperkuat klaim bahwa *due diligence* telah bergerak dari sekadar *soft law* menuju norma hukum kebiasaan internasional yang diakui secara luas.

Analisis lebih lanjut menunjukkan bahwa posisi hukum Indonesia terhadap prinsip *due diligence* mulai memperoleh penguatan normatif melalui kerangka kebijakan nasional. Dokumen Strategi Keamanan Siber Nasional (Stranas KS) yang disusun oleh Badan Siber dan Sandi Negara (Badan Siber dan Sandi

Negara (BSSN), 2020) menegaskan pentingnya tanggung jawab negara dalam menjamin ruang siber yang aman, andal, dan bertanggung jawab. Walaupun terminologi *due diligence* belum disebut secara eksplisit, semangat prinsip tersebut tercermin dalam pilar "tata kelola keamanan siber nasional" dan "ketahanan infrastruktur informasi kritis," yang mengharuskan negara melakukan tindakan preventif terhadap penyalahgunaan sistem nasional untuk menyerang pihak lain. Prinsip ini sejalan dengan konsep *due diligence* dalam hukum internasional yang menuntut negara mengambil langkah wajar untuk mencegah aktivitas berbahaya dari wilayahnya (Moynihan, 2023)

Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Undang-Undang Nomor 27, 2022) memperkuat basis hukum nasional dalam mendukung penerapan prinsip *due diligence*. UU ini memuat kewajiban negara dan penyelenggara sistem elektronik untuk menjaga keamanan data pribadi, termasuk kewajiban mencegah kebocoran, penyalahgunaan, dan serangan terhadap sistem digital. Dari sudut pandang hukum internasional, regulasi ini mencerminkan langkah konkret Indonesia dalam memenuhi sebagian unsur *due diligence*, terutama dalam aspek pencegahan pelanggaran lintas batas dan penguatan akuntabilitas hukum digital (Alramamneh & Abuanzeh, 2023). Walaupun belum secara eksplisit mengatur tanggung jawab negara terhadap *cyber* attacks, kombinasi antara Stranas KS dan UU PDP menunjukkan bahwa Indonesia tengah bergerak menuju implementasi prinsip *due diligence* dalam kerangka hukum nasional.

Sebagai bagian dari komunitas regional, Indonesia juga memiliki posisi strategis dalam kerangka ASEAN *Cybersecurity Cooperation Strategy* 2021–2025. Dokumen tersebut menegaskan komitmen negara-negara ASEAN terhadap prinsip "*responsible state behaviour in cyberspace*," yang sejalan dengan esensi *due diligence* dalam hukum internasional. Melalui forum seperti *ASEAN Ministerial Conference on Cybersecurity* (AMCC) dan *ASEAN Digital Ministers' Meeting* (ADGMIN), negara-negara anggota berupaya membangun kesamaan persepsi atas tanggung jawab negara di ruang siber, termasuk mekanisme berbagi informasi dan pencegahan serangan lintas batas (Egloff & Smeets, 2023).

Indonesia secara aktif berperan dalam inisiatif ini, baik sebagai tuan rumah diskusi kebijakan siber ASEAN maupun sebagai pengusul penguatan kerangka kerja hukum siber regional. Partisipasi aktif ini memperlihatkan bahwa upaya implementasi *due diligence* tidak hanya bersifat nasional, tetapi juga terintegrasi dalam komitmen kawasan. Pendekatan berbasis regional semacam ini penting untuk memperkuat posisi hukum Indonesia di forum internasional, sekaligus memperkaya proses kodifikasi norma kebiasaan global mengenai perilaku negara yang bertanggung jawab di dunia maya.

Hasil penelitian ini memiliki konsistensi dengan sejumlah studi sebelumnya. (Radanliev, 2024) menegaskan bahwa kapabilitas teknis dan kelembagaan negara menjadi faktor kunci keberhasilan penerapan *due diligence* di ranah siber, sejalan dengan temuan penelitian ini bahwa negara dengan infrastruktur siber kuat lebih siap memenuhi kewajiban tersebut. Penelitian ini juga memperkuat temuan (Adeyeri & Abroshan, 2024) mengenai kecenderungan negara berkembang menunda adopsi

prinsip ini karena keterbatasan sumber daya. Sebaliknya, penelitian ini menunjukkan bahwa Indonesia telah memulai proses internalisasi norma melalui kebijakan nasional seperti Stranas KS dan UU PDP 2022. Berbeda dengan (Gstrein & Beaulieu, 2022) yang menilai sulitnya penerapan prinsip hukum tradisional di ranah digital, hasil penelitian ini menegaskan bahwa pembaruan hukum nasional dan koordinasi regional melalui ASEAN dapat menjadi instrumen efektif untuk mengoperasionalkan *due diligence* di dunia maya.

Meski begitu, penelitian ini memiliki sejumlah keterbatasan. Pertama, pendekatan normatif-yuridis tidak mencakup pengujian empiris terhadap efektivitas implementasi prinsip *due diligence* di tingkat praktis. Kedua, fokus penelitian terbatas pada Indonesia dan lima negara representatif tanpa memperluas perbandingan ke negara-negara ASEAN lainnya yang menghadapi tantangan serupa. Ketiga, penelitian ini bergantung pada data sekunder, sehingga keterbatasan akses terhadap data primer menjadi kendala dalam memperdalam analisis kebijakan domestik.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk melakukan studi empiris yang menilai implementasi *due diligence* di negara-negara berkembang melalui wawancara dengan pembuat kebijakan dan lembaga keamanan siber. Analisis komparatif antarnegara ASEAN juga penting untuk memahami dinamika regional dalam pembentukan norma hukum siber bersama.

Dengan demikian, penelitian ini menegaskan bahwa implementasi prinsip *due diligence* dalam keamanan siber bukan hanya isu normatif, tetapi juga terkait erat dengan kapasitas nasional, dinamika geopolitik, dan komitmen regional. Indonesia memiliki peluang besar untuk memperkuat posisinya melalui pembaruan regulasi nasional, peningkatan kapasitas kelembagaan, dan partisipasi aktif dalam pembentukan norma hukum internasional yang lebih responsif terhadap tantangan ruang siber global

IV. KESIMPULAN

Penelitian ini menegaskan bahwa prinsip *due diligence* merupakan fondasi penting dalam hukum internasional kontemporer untuk menilai kewajiban negara dalam mencegah aktivitas siber yang berpotensi merugikan negara lain. Melalui pendekatan normatif dan analisis kebijakan dari berbagai negara, ditemukan bahwa masih terdapat kesenjangan signifikan antara eksistensi prinsip ini dalam doktrin hukum internasional dengan implementasinya dalam praktik negara, terutama di negara-negara berkembang seperti Indonesia. Ketidakhadiran instrumen hukum internasional yang mengikat dan belum meratanya kapasitas siber di tingkat nasional menjadi hambatan utama dalam pelaksanaan prinsip ini secara efektif dan konsisten. Selain itu, dinamika geopolitik dan interpretasi yang beragam terhadap batas kewajiban negara turut mempersulit terciptanya standar global yang dapat diadopsi secara luas.

Kontribusi utama dari penelitian ini terletak pada pemetaan konsep, identifikasi celah normatif, dan perumusan rekomendasi praktis mengenai penerapan prinsip *due diligence* dalam tata kelola keamanan siber. Dengan menyoroti posisi Indonesia, penelitian ini tidak hanya memberikan gambaran atas

tantangan yang dihadapi, tetapi juga membuka ruang bagi pembentukan strategi kebijakan yang lebih responsif terhadap kewajiban internasional. Pemahaman dan penerapan prinsip ini diharapkan tidak hanya meningkatkan legitimasi posisi hukum Indonesia di ranah global, tetapi juga memperkuat sistem pertahanan siber nasional dalam menghadapi ancaman digital lintas batas yang kian kompleks dan disruptif. Penelitian ini menegaskan posisi prinsip *due diligence* sebagai jembatan antara kewajiban hukum dan kapasitas institusional negara. Implementasi prinsip ini akan menentukan legitimasi Indonesia dalam tata kelola siber global.

REFERENCES

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information (Switzerland)*, *15*(11). https://doi.org/10.3390/info15110682

Agir, S., Derin-Gure, P., & Senturk, B. (2023). Farmers' perspectives on challenges and opportunities of agrivoltaics in Turkiye: An institutional perspective. *Renewable Energy*, *212*, 35–49. https://doi.org/10.1016/j.renene.2023.04.137

Alramamneh, I. M., & Abuanzeh, A. (2023). International and National Procedural Framework for Combating Cybercrime. *International Journal of Cyber Criminology*, *17*(2), 330–349. https://doi.org/10.5281/zenodo.4766719

Asmare, F. M., & Ayalew, L. G. (2023). Security challenges in the transition to 4G mobile systems in developing countries. *Cogent Engineering*, *10*(1). https://doi.org/10.1080/23311916.2023.2166214

Badan Siber dan Sandi Negara (BSSN). (2020). *Strategi Keamanan Siber Nasional (Stranas KS)*. https://bssn.go.id/

Bannelier, K. (2024). *Due diligence* as a cardinal principle in the fight against malicious cyber activities. *Global Cybersecurity and International Law*, 44–62. https://doi.org/10.4324/9781003344124-4

Cinini, S. F., Ehiane, S. O., Osaye, F. J., & Irewunmi, B. A. (2023). The trends of cybersecurity and its emerging challenges in Africa. *Cybercrime and Challenges in South Africa*, 75–106. https://doi.org/10.1007/978-981-99-3057-9_4

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, *46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117

Fajri, K. S. Al, & Harwahyu, R. (2024). Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(2), 498–506. https://doi.org/10.57152/malcom.v4i2.1245

Government of Estonia. (2023). *Cybersecurity Act*. https://www.mkm.ee/en/

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy and Technology*, *35*(1). https://doi.org/10.1007/s13347-022-00497-4

Guo, D., Chen, H., Wu, R., & Wang, Y. (2023). AIGC challenges and opportunities related to public safety: A case study of ChatGPT. *Journal of Safety Science and Resilience*, *4*(4), 329–339. https://doi.org/10.1016/j.jnlssr.2023.08.001

Gustafsson, M. T., Schilling-Vacaflor, A., & Lenschow, A. (2023). Foreign corporate accountability: The contested institutionalization of mandatory *due diligence* in France and Germany. *Regulation and*

Governance, *17*(4), 891–908. https://doi.org/10.1111/rego.12498

Imoize, A. L., Balas, V. E., Solanki, V. K., Lee, C. C., & Obaidat, M. S. (2023). Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things. *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things*, 1–471. https://doi.org/10.1201/9781003370321

International Law Commission (ILC). (2022). *Draft conclusions on identification of customary international law, with commentaries.* United Nations.

Islam, E., Rudolph, C., & Oliver, G. (2025). Managing cyber harm: a survey of challenges, practices, and opportunities. *Information Security Journal*. https://doi.org/10.1080/19393555.2025.2484348

Katagiri, N. (2024). Defending medical facilities from cyber attacks: critical issues with the principle of *due diligence* in international law. *International Review of Law, Computers and Technology*, *38*(1), 1–20. https://doi.org/10.1080/13600869.2023.2183449

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, *56*, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Malhotra, A., Mathur, A., Diddi, S., & Sagar, A. D. (2022). Building institutional capacity for addressing climate and sustainable development goals: achieving energy efficiency in India. *Climate Policy*, *22*(5), 652–670. https://doi.org/10.1080/14693062.2021.1984195

Moynihan, H. (2023). Unpacking *due diligence* in cyberspace. *Journal of Cyber Policy*, *8*(1), 4–25. https://doi.org/10.1080/23738871.2023.2250358

Nowak, D., & Distel, B. (2024). Trust in Times of Cyber Crisis: Understanding Organizational Trust Repair in the Public Sector. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *14841 LNCS*, 134–149. https://doi.org/10.1007/978-3-031-70274-7_9

Open-Ended Working Group. (2023). *Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://www.un.org/disarmament/

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. https://doi.org/10.1080/23742917.2024.2312671

Sachoulidou, A. (2023). Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-023-09347-w

Sankaran, V., & Church, C. (2023). The Ties that Bind Us: An Empirical, Clinical, and Constitutional Argument Against Terminating Parental Rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4397994

Schilling-Vacaflor, A., & Gustafsson, M. T. (2024). Towards More Sustainable Global Supply Chains? Company Compliance with new Human Rights and Environmental *Due diligence* Laws. *Environmental Politics*, *33*(3), 422–443. https://doi.org/10.1080/09644016.2023.2221983

Schilling-Vacaflor, A., & Lenschow, A. (2023). Hardening foreign corporate accountability through mandatory *due diligence* in the European Union? New trends and persisting challenges. *Regulation and Governance*, *17*(3), 677–693. https://doi.org/10.1111/rego.12402

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information*

Integration, *36*. https://doi.org/10.1016/j.jii.2023.100520

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology and Politics*, *20*(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *37*. https://doi.org/10.1016/j.ijcip.2021.100505

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information (Switzerland)*, *13*(3). https://doi.org/10.3390/info13030146

Undang-Undang Nomor 27. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

United Nations Group of Governmental Experts. (2021). *Report on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)*. https://www.un.org/disarmament/

United States Government. (2022). *National Cyber Strategy of the United States of America*. https://www.whitehouse.gov/

Wang, J., Yang, J., & Yang, L. (2023). Do natural resources play a role in economic development? Role of institutional quality, trade openness, and FDI. *Resources Policy*, *81*. https://doi.org/10.1016/j.resourpol.2023.103294

Wilhelm, M. (2024). Mandatory *due diligence* legislation: a paradigm shift for the governance of sustainability in global value chains? *Journal of International Business Policy*. https://doi.org/10.1057/s42214-024-00193-4

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. https://doi.org/10.1007/s10207-021-00545-8

Żuk, P., & Żuk, P. (2024). Ecology for the rich? Class aspects of the green transition and the threat of right-wing populism as a reaction to its costs in Poland. *Sustainability: Science, Practice, and Policy*, *20*(1). https://doi.org/10.1080/15487733.2024.2351231