Aliansi : Jurnal Hukum, Pendidikan dan Sosial Humaniora
Volume. 2, Nomor. 4 Juli 2025
e-ISSN: 3031-9706; p- ISSN: 3031-9684, Hal 262-277
DOI: https://doi.org/10.62383/aliansi.v2i4.1116
Available online at: https://journal.appihi.or.id/index.php/Aliansi

Strategi *Detterence* Siber Indonesia terhadap Ancaman *Proxy State Actor*

Aminarti Fithri Amalia[1*], Wira Atman[2]
[1-2] Universitas Hasanudin, Indonesia

Alamat: Jalan Perintis Kemerdekaan IV Tamalanrea, Kota: Makassar Kode Pos: 90245
Provinsi: Sulawesi Selatan
*Korespondensi penulis: aminarty.amalia@gmail.com**

Abstract. *Advances in information technology have increased the country's vulnerability to cyber threats, including attacks by proxy state actors that are difficult to track and account for. Indonesia as a developing country faces challenges in formulating an effective cyber defense strategy. This study aims to analyze Indonesia's cyber deterrence strategy in dealing with proxy state actor threats, and to compare it with the approaches taken by Singapore and South Korea. The research method used is a qualitative study with a comparative approach, examining policies, institutional capacity, and the effectiveness of strategy implementation in each country. Initial findings indicate that Indonesia is still in the early stages of developing an integrated cyber deterrence strategy, especially in terms of attribution, cyber diplomacy, and strengthening national capacity. Singapore and South Korea have implemented a more systematic approach, including regional cooperation and cross-sector policy integration. The results of this study are expected to contribute to the formulation of national policies in strengthening Indonesia's digital resilience and sovereignty*.

Keywords: *Cyber deterrence, Indonesia, Proxy State Actor, South Korea, Singapore*.

Abstrak. Kemajuan teknologi informasi telah meningkatkan kerentanan negara terhadap ancaman di ranah siber, termasuk serangan oleh proxy state actor yang sulit dilacak dan dipertanggungjawabkan. Indonesia sebagai negara berkembang menghadapi tantangan dalam merumuskan strategi pertahanan siber yang efektif. Penelitian ini bertujuan untuk menganalisis strategi deterrence siber Indonesia dalam menghadapi ancaman proxy state actor, serta membandingkannya dengan pendekatan yang diambil oleh Singapura dan Korea Selatan. Metode penelitian yang digunakan adalah studi kualitatif dengan pendekatan komparatif, mengkaji kebijakan, kapasitas kelembagaan, serta efektivitas implementasi strategi pada masing-masing negara. Temuan awal menunjukkan bahwa Indonesia masih berada pada tahap awal pengembangan strategi deterrence siber yang terintegrasi, terutama dalam aspek atribusi, diplomasi siber, dan penguatan kapasitas nasional. Singapura dan Korea Selatan telah menerapkan pendekatan yang lebih sistematis, termasuk kerjasama regional dan integrasi kebijakan lintas sektor. Hasil studi ini diharapkan memberikan kontribusi bagi perumusan kebijakan nasional dalam memperkuat ketahanan dan kedaulatan digital Indonesia.

Kata kunci: Eterrence Siber, Indonesia, Proxy State Actor, Korea Selatan, Singapura.

1. LATAR BELAKANG

Perkembangan teknologi informasi telah mengubah lanskap keamanan nasional secara drastis. Di era digital ini, ruang siber menjadi arena strategis yang digunakan negara maupun aktor non-negara untuk melancarkan operasi yang tidak selalu terlihat secara kasat mata, namun memiliki dampak besar terhadap stabilitas negara. Ancaman siber, yang awalnya dianggap sebagai gangguan teknis biasa, kini berkembang menjadi instrumen geopolitik yang kompleks. Salah satu bentuk ancaman paling berbahaya adalah keterlibatan *proxy state actor* dalam serangan siber, yaitu aktor non-negara yang secara langsung atau tidak langsung mendapat dukungan dari suatu negara untuk melakukan tindakan ofensif di dunia maya. Serangan jenis ini sangat sulit diatribusikan dan menimbulkan dilema hukum dan diplomatik bagi negara yang menjadi korban (Galang Ramadhan, 2025).

Received: Mei 27, 2025; Revised: Juni 07, 2025; Accepted: Juni 21, 2025; Online Available: Juni 24, 2025

Indonesia sebagai negara berkembang yang sedang mengalami percepatan transformasi digital, menjadi sasaran potensial dari ancaman-ancaman ini. Dalam beberapa tahun terakhir, Indonesia mengalami serangkaian insiden siber yang signifikan, mulai dari kebocoran data penduduk, serangan terhadap sistem layanan publik, peretasan situs institusi pemerintah, hingga penetrasi terhadap infrastruktur digital sektor keuangan dan energi. Pada tahun 2022, publik dikejutkan dengan kasus kebocoran data 1,3 miliar SIM card, yang diduga berasal dari sistem registrasi pelanggan milik operator nasional. Kasus serupa terus berulang, termasuk peretasan situs Komisi Pemilihan Umum (KPU), sistem eHAC, dan gangguan terhadap layanan digital milik PLN dan Pertamina. Sebagian besar serangan ini menunjukkan pola teknis yang kompleks dan canggih, sehingga memunculkan dugaan kuat bahwa serangan tersebut dilakukan oleh kelompok peretas yang terorganisasi, kemungkinan besar berkaitan dengan aktor proksi negara asing (Subrata et al., 2020).

Masalah utama yang dihadapi Indonesia bukan hanya pada sisi kerentanannya terhadap serangan, tetapi juga pada lemahnya kemampuan atribusi. Sampai saat ini, Indonesia belum memiliki sistem atau protokol yang mumpuni untuk mengidentifikasi secara sah dan akurat siapa pelaku di balik serangan siber tersebut. Ketiadaan kapasitas atribusi ini berdampak langsung pada lemahnya respons negara—baik secara hukum, diplomatik, maupun teknis. Tanpa kemampuan untuk membuktikan pelaku serangan, Indonesia berada dalam posisi defensif yang lemah dan rentan terhadap eksploitasi berulang.

Pendekatan Indonesia dalam menangani serangan siber masih bersifat reaktif, administratif, dan kurang strategis. Meski pemerintah telah membentuk Badan Siber dan Sandi Negara (BSSN) serta menetapkan Perpres No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital, implementasi kebijakan tersebut belum mampu menghadirkan efek jera atau efek penangkalan (*deterrent effect*) terhadap pelaku serangan. Hal ini terjadi karena kebijakan dan institusi yang ada belum sepenuhnya terintegrasi dalam sistem pertahanan nasional, serta belum mampu menghadapi kompleksitas ancaman dari aktor proksi (Vimy et al., 2022).

Negara-negara seperti Singapura dan Korea Selatan sudah lebih dahulu menyadari pentingnya strategi *cyber deterrence* dalam menjaga kedaulatan digital. Singapura, dengan pengesahan *Cybersecurity Act* tahun 2018 dan pembentukan *Cyber Security Agency* (CSA), telah membangun sistem pertahanan siber nasional yang terintegrasi dan berorientasi pada pencegahan. Korea Selatan bahkan mengembangkan unit *cyber command* militer, sebagai bagian dari strategi kombinasi antara *deterrence by denial* dan *deterrence by punishment*, terutama untuk menghadapi ancaman dari Korea Utara.

Indonesia menghadapi tantangan besar. Di satu sisi, tekanan untuk melindungi infrastruktur digital dan data warganya semakin tinggi; di sisi lain, kemampuan dan sistem nasional untuk menangkal ancaman belum memadai. Ketika serangan yang datang bersumber dari *proxy state actor*, pendekatan konvensional tidak lagi cukup. Diperlukan pendekatan strategis berbasis teori *cyber deterrence* yang komprehensif—yang tidak hanya mengandalkan pertahanan pasif, tetapi juga membangun kapasitas atribusi, kekuatan hukum, dan kerja sama internasional.

Peneliltian ini berangkat dari urgensi tersebut. Penelitian ini berupaya untuk mengevaluasi kesiapan Indonesia dalam menghadapi serangan siber yang dimotori oleh aktor proksi negara asing, serta membandingkannya dengan pendekatan yang dilakukan oleh Singapura dan Korea Selatan. Harapannya, studi ini dapat memberikan gambaran tentang di mana posisi Indonesia saat ini, serta menawarkan rekomendasi berbasis praktik terbaik (*best practices*) dari negara lain yang telah lebih dahulu membangun sistem *cyber deterrence* yang efektif.

Dengan meningkatnya kompleksitas ancaman siber global, Indonesia tidak bisa lagi bertahan dalam posisi reaktif. Tanpa adanya strategi yang jelas, sistematis, dan terukur, Indonesia akan terus berada dalam posisi rentan dalam menghadapi agresi digital, baik dari aktor negara maupun non-negara. Maka dari itu, pembangunan strategi *cyber deterrence* nasional menjadi kebutuhan mendesak yang tidak bisa ditunda. Diharapkan hasil penelitian ini tidak hanya memberikan kontribusi akademik terhadap pengembangan literatur di bidang keamanan siber, tetapi juga menawarkan rekomendasi kebijakan yang aplikatif bagi penguatan ketahanan siber nasional. Dalam jangka panjang, upaya ini diharapkan dapat memperkuat posisi Indonesia dalam menjaga kedaulatan digital dan stabilitas keamanan nasional di tengah dinamika geopolitik global yang semakin kompleks.

Penelitian ini berangkat dari premis bahwa ancaman siber modern, terutama yang bersumber dari *proxy state actor*, menuntut negara untuk mengembangkan strategi pertahanan berbasis teori yang kuat dan relevan. Dua teori utama yang digunakan dalam penelitian ini adalah Teori Penangkalan Siber (Cyber Deterrence Theory) dan Teori Aktor Proksi dalam Hubungan Internasional (Proxy Actor Theory). Kedua teori ini membentuk fondasi dalam menganalisis efektivitas kebijakan Indonesia dan membandingkannya dengan strategi Singapura dan Korea Selatan.

Teori Penangkalan Siber (Cyber Deterrence Theory)

Teori penangkalan (*deterrence*) berasal dari tradisi studi militer dan hubungan internasional, berkembang pada era Perang Dingin sebagai strategi untuk mencegah agresi, khususnya serangan nuklir, melalui ancaman pembalasan. Dalam konteks modern, teori ini mengalami adaptasi ke dalam ranah digital sebagai *cyber deterrence theory*, yaitu bagaimana negara mencegah serangan siber melalui ancaman hukuman, pengurangan insentif serangan, atau penegakan norma internasional. Dalam kerangka ini, Stefan Soesanto (2022) mengemukakan enam mekanisme utama penangkalan siber *deterrence by denial*, *deterrence by punishment*, *delegitimization*, *entanglement*, *reputation*, dan *cross-domain deterrence*. Namun dalam konteks Indonesia, paling relevan untuk dianalisis adalah empat mekanisme utama pertama:

- **Deterrence by Denial**

  Pendekatan ini bertujuan membuat serangan menjadi tidak efektif, dengan memperkuat sistem pertahanan informasi, deteksi dini, serta kemampuan respons cepat. Di Indonesia, mekanisme ini tercermin dalam upaya BSSN (Badan Siber dan Sandi Negara) untuk membangun proteksi terhadap Infrastruktur Informasi Vital Nasional. Namun kenyataannya, kasus kebocoran data besar seperti eHAC dan SIM card 1,3 miliar nomor menunjukkan bahwa mekanisme denial belum berjalan optimal. Infrastruktur digital nasional masih rentan karena keterbatasan kapasitas teknis, sumber daya manusia, dan koordinasi antarlembaga.

- **Deterrence by Punishment**

  Mekanisme ini mengandalkan ancaman balasan terhadap pelaku serangan, misalnya melalui sanksi hukum, tindakan balasan siber, atau diplomasi koersif. Tantangannya di Indonesia adalah lemahnya kemampuan atribusi; negara tidak mampu mengidentifikasi dengan pasti siapa pelaku di balik serangan. Akibatnya, Indonesia tidak memiliki dasar untuk menjatuhkan hukuman secara sah, baik secara nasional maupun internasional. Hingga kini, tidak ada kerangka hukum atau prosedur operasional tetap yang memungkinkan Indonesia melakukan respons ofensif atau bahkan sanksi diplomatik terhadap pelaku serangan yang terindikasi sebagai *proxy state actor*.

- **Delegitimization**

  Upaya ini berkaitan dengan mempermalukan dan mengisolasi pelaku melalui pengungkapan publik atau kerja sama internasional. Sayangnya, Indonesia masih pasif dalam forum-forum diplomasi siber global, sehingga tidak memiliki kapasitas atau

reputasi untuk menekan aktor asing melalui jalur normatif. Belum adanya keterlibatan kuat Indonesia dalam konvensi seperti *Budapest Convention on Cybercrime* membuat strategi delegitimasi ini belum dapat dijalankan secara maksimal.

- **Entanglement dan Reputation**

  Negara yang memiliki hubungan diplomatik dan ekonomi yang erat dengan pihak luar cenderung lebih terlindungi, karena serangan terhadapnya juga dapat merugikan pelaku. Namun posisi Indonesia dalam hal ini lemah. Reputasi Indonesia di bidang keamanan siber masih belum terbentuk kuat, dan belum ada insentif bagi negara atau aktor lain untuk menahan diri dalam menyerang sistem siber Indonesia. Bahkan kerja sama sektor privat dan publik dalam menjaga keamanan digital masih terbatas.

Teori deterrence pertama kali dikembangkan oleh Cesare Becaria (Italia) dan Jeremy Bentham (Inggris) pada abad ke-18. Penelitian ini berfokus terutama pada dua mekanisme utama: denial dan punishment. Di Indonesia bentuk deterrence by denial tercermin dalam peran Badan Siber dan Sandi Negara (BSSN) dalam melindungi infrastruktur vital. Namun, keterbatasan teknologi, sumber daya manusia, dan koordinasi antar-lembaga membuat daya tangkal ini masih lemah. Sementara itu, pendekatan punishment belum berkembang signifikan karena belum ada instrumen hukum maupun kapasitas ofensif yang memadai. Hal ini berbeda dengan Singapura yang menerapkan *Cybersecurity Act 2018* dan Korea Selatan yang memiliki unit cyber military command aktif, sehingga dapat menunjukkan efek tangkal yang lebih kuat. Teori deterrence pertama kali dikembangkan oleh Cesare Becaria (Italia) dan Jeremy Bentham (Inggris) pada abad ke-18. Efektivitas teori deterrence sangat bergantung pada beberapa faktor:

- Kemampuan atribusi yang valid, agar hukuman bisa diberikan pada pihak yang tepat.
- Kapabilitas teknis dalam mendeteksi, menganalisis, dan memulihkan serangan.
- Koherensi kebijakan antara lembaga sipil dan militer.
- Respon diplomatik dan hukum yang konsisten.

Tanpa pemenuhan faktor-faktor tersebut, strategi deterrence tidak hanya tidak efektif, tetapi juga berpotensi kontraproduktif karena membuka celah eksploitasi berulang oleh aktor yang sama.

Teori Aktor Proksi dalam Hubungan Internasional (Proxy Actor Theory)

Aktor proksi atau *proxy actors* dalam hubungan internasional merupakan entitas yang bertindak atas nama negara, baik secara langsung (dengan dukungan) maupun tidak langsung (dengan pembiaran atau kesamaan tujuan), untuk mencapai kepentingan strategis tanpa keterlibatan resmi negara sponsor. *Proxy state actor* sering digunakan sebagai alat perang tidak

langsung yang sulit ditelusuri, murah biayanya, dan memiliki risiko politik rendah bagi negara sponsor. Menurut (Darumaya et al., 2023), *proxy cyber actors* dapat dibagi menjadi tiga kategori:

- State-Directed Proxies – aktor yang mendapatkan perintah langsung dari negara.
- State-Sanctioned Proxies – kelompok independen yang didukung logistik atau dibiarkan beroperasi oleh negara.
- State-Independent Proxies – aktor non-negara yang bertindak atas dasar ideologi atau motif finansial, namun menguntungkan suatu negara.

Keberadaan *proxy actor* memperlemah efektivitas strategi punishment dalam deterrence karena:

- Sulitnya atribusi langsung kepada negara asal.
- Ketiadaan kerangka hukum internasional yang jelas untuk menindak negara yang "memfasilitasi" kelompok tersebut.
- Risiko escalation control yang tinggi bila suatu negara membalas ke negara sponsor berdasarkan dugaan yang tidak pasti.

Peran *proxy actor* dianalisis dalam konteks respons Indonesia, Singapura, dan Korea Selatan terhadap berbagai bentuk agresi siber. Singapura dan Korea Selatan, misalnya, memiliki sistem deteksi dan kerja sama regional yang memungkinkan mereka mempersempit ruang gerak aktor proksi. Sebaliknya, Indonesia belum memiliki sistem manajemen insiden nasional yang terintegrasi, sehingga respons terhadap serangan siber bersifat reaktif dan parsial. Implikasi dari teori ini adalah perlunya strategi penangkalan yang tidak hanya fokus pada pelaku serangan langsung, tetapi juga mekanisme diplomatik dan legal untuk menekan negara yang diduga melindungi atau membiayai aktor proksi (Nefo et al., 2025).

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam studi ini adalah metode kualitatif-komparatif dengan pendekatan studi kasus. Penelitian ini membandingkan strategi deterrence siber Indonesia terhadap ancaman *proxy state actor* dengan strategi yang diterapkan oleh Singapura dan Korea Selatan. Data dikumpulkan melalui studi literatur terhadap dokumen kebijakan, laporan lembaga pemerintah dan non-pemerintah, serta publikasi ilmiah terkait keamanan siber. Teknik pengumpulan data menggunakan dokumentasi dan wawancara semi-terstruktur dengan informan ahli di bidang keamanan siber dan hubungan internasional.

Analisis data dilakukan dengan teknik analisis isi dan pendekatan tematik untuk mengidentifikasi pola, perbedaan, dan kesamaan strategi yang digunakan ketiga negara. Model analisis yang digunakan mengacu pada kerangka mekanisme deterrence siber menurut (Suwarno & Widodo, 2022)yang mencakup deterrence by denial, punishment, delegitimization, reputation, entanglement, dan cross-domain. Interpretasi hasil disajikan secara deskriptif-kritis untuk memberikan pemahaman yang komprehensif terhadap efektivitas strategi masing-masing negara.

3. HASIL DAN PEMBAHASAN

Pengertian Karakter Religius Secara Etimologi secara etimologi, kata "karakter" berasal

Global Ancaman Siber dan Peran Proxy State Actor

Dalam dua dekade terakhir dunia telah mengalami lonjakan eksponensial dalam perkembangan teknologi digital, yang turut mengubah wajah ancaman keamanan di tingkat global. Ruang siber kini tidak hanya menjadi arena pertukaran informasi dan aktivitas ekonomi, tetapi juga telah berkembang menjadi medan pertempuran strategis antarnegara. Serangan siber menjadi instrumen baru dalam konflik geopolitik, karena kemampuannya menyusup ke dalam sistem suatu negara tanpa perlu intervensi fisik, serta memberikan keuntungan bagi aktor penyerang melalui kerahasiaan, efisiensi biaya, dan ambiguitas hukum. Di antara ragam aktor dalam serangan siber ini, *proxy state actor* atau aktor proksi negara menjadi elemen yang paling kompleks dan berbahaya, terutama karena keberadaan mereka sulit dibuktikan secara langsung, namun berkaitan erat dengan kepentingan strategis negara sponsor (Ginanjar, 2022).

Proxy state actor merujuk pada kelompok atau individu non-negara yang bertindak atas dukungan, izin, atau pembiaran negara tertentu dalam menjalankan serangan siber terhadap pihak ketiga. Dukungan ini bisa berupa pelatihan, perlindungan hukum, infrastruktur digital, atau bahkan dana operasional. Berbeda dengan aktor non-negara biasa seperti peretas kriminal (cybercriminal), aktor proksi memiliki tujuan politis yang selaras dengan negara sponsor dan sering menjadi alat dalam konflik asimetris. Dengan menggunakan aktor-aktor ini, negara sponsor bisa menghindari tanggung jawab langsung atas serangan, sekaligus menguji ketahanan lawan tanpa harus terlibat dalam konflik terbuka (Ginanjar, 2022).

Fenomena penggunaan *proxy actor* dalam ranah siber telah menjadi isu sentral dalam kajian keamanan internasional. Negara-negara besar seperti Rusia, China, Iran, dan Korea Utara diduga kuat telah menggunakan strategi ini untuk menyerang negara-negara Barat, terutama Amerika Serikat dan sekutunya. Salah satu contoh paling terkenal adalah serangan

terhadap Komite Nasional Partai Demokrat AS (DNC) pada tahun 2016 yang dikaitkan dengan kelompok peretas APT 28 atau "Fancy Bear" yang memiliki hubungan dengan intelijen militer Rusia. Demikian pula dengan kelompok Lazarus yang berbasis di Korea Utara, yang terlibat dalam serangan ransomware WannaCry dan berbagai peretasan terhadap bank dan perusahaan teknologi, serta APT 41 yang diduga terhubung dengan Kementerian Keamanan Negara China. Aktor-aktor ini secara teknis tidak berstatus sebagai bagian resmi dari militer atau pemerintah, namun pola aktivitas, target, dan perlindungan yang mereka terima memperlihatkan korelasi langsung dengan kebijakan luar negeri negara sponsor (Wibowo et al., 2024).

Indonesia sebagai negara berkembang dengan pertumbuhan digital yang tinggi, tidak terlepas dari ancaman yang sama. Beberapa insiden siber yang terjadi di Indonesia, seperti kebocoran data pribadi dari instansi pemerintah, peretasan situs lembaga strategis, dan penyusupan terhadap sistem pelayanan publik, menunjukkan adanya aktivitas aktor siber tingkat tinggi yang tidak selalu dapat dikategorikan sebagai kriminal biasa. Tantangan utamanya adalah ketidakmampuan otoritas nasional untuk mengidentifikasi dan membuktikan dengan akurat siapa aktor di balik serangan tersebut. Hal ini mengindikasikan kemungkinan keterlibatan *proxy actor* asing yang menyamarkan operasinya melalui jaringan server internasional, malware yang sulit dilacak, serta pemanfaatan infrastruktur cloud yang tersebar global (Heryadi et al., 2024).

Keberadaan *proxy state actor* mempersulit penerapan teori *cyber deterrence*, terutama mekanisme *deterrence by punishment* yang mengandalkan kemampuan atribusi untuk membalas serangan. Tanpa bukti jelas siapa pelakunya, negara korban tidak dapat menerapkan hukuman yang sah secara hukum internasional. Oleh karena itu, beberapa negara seperti Amerika Serikat mulai mengembangkan strategi *persistent engagement* dan *defend forward*, yakni dengan aktif mencari dan mengganggu infrastruktur siber musuh secara proaktif. Strategi ini memerlukan kapabilitas tinggi dalam atribusi, kerja sama intelijen internasional, serta kerangka hukum nasional yang memungkinkan aksi pre-emptive di dunia maya (Bhakti et al., 2024).

Berbeda dengan negara-negara besar yang memiliki sumber daya dan otoritas untuk menjalankan strategi ofensif, negara seperti Indonesia berada pada posisi yang lebih rentan. Struktur kelembagaan yang masih berkembang, keterbatasan dalam teknologi forensik digital, serta belum terintegrasinya kebijakan keamanan siber lintas sektor menjadikan Indonesia sulit dalam menghadapi ancaman *proxy actor*. Untuk mengatasi hal ini, diperlukan strategi nasional yang tidak hanya bersifat defensif, tetapi juga mencakup penguatan sistem atribusi, kerja sama

internasional dalam penegakan hukum siber, serta peningkatan kapasitas lembaga seperti BSSN dalam melakukan deteksi dini dan analisis insiden (Ma'aliya et al., 2023).

Dari hasil pengamatan terhadap tren serangan global dan regional, terlihat bahwa negara-negara yang berhasil menahan serangan *proxy actor* adalah mereka yang memiliki sistem koordinasi nasional yang kuat, jaringan kerja sama regional yang aktif, serta strategi pencegahan yang terintegrasi dengan diplomasi siber dan penguatan norma internasional. Studi perbandingan dengan Singapura dan Korea Selatan dalam penelitian ini menunjukkan bahwa pendekatan berbasis kebijakan strategis dan kolaboratif terbukti lebih efektif dalam mengelola ancaman kompleks dari aktor proksi. pemahaman terhadap ancaman global dan peran *proxy state actor* menjadi landasan dalam merumuskan kebijakan penangkalan siber Indonesia ke depan. Tanpa pendekatan yang strategis dan berbasis bukti, Indonesia berisiko terus menjadi target empuk dalam konflik siber global yang semakin sulit diprediks (Ma'aliya et al., 2023).

Strategi Singapura dalam Menangkal Ancaman Siber

Singapura merupakan salah satu negara di kawasan Asia Tenggara yang dianggap paling siap dan maju dalam menghadapi ancaman siber, termasuk yang berasal dari *proxy state actor*. Sebagai negara kota dengan ketergantungan tinggi pada teknologi informasi, Singapura mengadopsi pendekatan yang komprehensif dan terintegrasi dalam membangun keamanan sibernya. Strategi ini tidak hanya menekankan pada aspek teknis, tetapi juga kelembagaan, hukum, diplomasi, dan partisipasi publik. Pendekatan ini menjadikan Singapura sebagai model negara yang berhasil mengimplementasikan *cyber deterrence* secara nyata dan terstruktur.

Singapura juga menerapkan *deterrence by delegitimization* dan reputasi melalui kerja sama regional dan global yang intensif. Singapura aktif dalam ASEAN Cybersecurity Cooperation Strategy dan berbagai forum internasional seperti United Nations Group of Governmental Experts (UNGGE) dan Global Forum on Cyber Expertise (GFCE). Dalam forum-forum ini, Singapura memperjuangkan norma dan aturan perilaku negara di dunia maya, serta mendorong penegakan hukum internasional terhadap aktor siber yang berbahaya. Strategi ini membantu membangun citra bahwa serangan terhadap Singapura tidak hanya akan dihadapi secara teknis, tetapi juga dengan tekanan diplomatik dan eksposur reputasi global.

Singapura memiliki sejumlah inisiatif penting seperti *Cybersecurity Labelling Scheme (CLS)* untuk perangkat IoT, *cybersecurity exercises* nasional seperti Exercise Cyber Star, dan investasi besar dalam pengembangan tenaga profesional siber melalui lembaga pendidikan serta program *SkillsFuture*. Semua inisiatif ini menunjukkan bahwa Singapura menempatkan keamanan siber sebagai bagian dari kebijakan publik, bukan hanya isu teknologi. Ketahanan

siber yang tinggi juga ditopang oleh kerja sama antara sektor publik dan swasta, terutama dalam hal pelaporan insiden, pengujian kerentanan, dan berbagi informasi ancaman (*threat intelligence*). CSA menjalin kemitraan dengan perusahaan teknologi, operator jaringan, dan institusi keuangan untuk memastikan adanya ekosistem pertahanan siber yang kolaboratif (Darumaya et al., 2023).

Strategi Korea Selatan dalam Menghadapi Serangan Proksi

Korea Selatan merupakan salah satu negara yang paling rentan terhadap ancaman siber, terutama yang berasal dari Korea Utara. Negara tersebut menjadi sasaran utama berbagai bentuk serangan siber, mulai dari pencurian data hingga sabotase sistem infrastruktur vital. Ancaman ini sebagian besar dilakukan oleh kelompok *proxy state actor* yang diyakini memiliki keterkaitan langsung dengan rezim Korea Utara, seperti Lazarus Group dan APT37. Dalam menghadapi realitas ancaman ini, Korea Selatan mengembangkan strategi keamanan siber yang tidak hanya berfokus pada pertahanan pasif, tetapi juga mencakup elemen penyerangan terbatas, diplomasi, dan kerja sama internasional. Strategi ini merupakan bentuk nyata dari pendekatan *cyber deterrence* yang holistik dan berorientasi pada kesiapsiagaan nasional.

Kunci dari strategi Korea Selatan adalah integrasi antara aspek sipil dan militer dalam sistem keamanan sibernya. Pemerintah Korea Selatan membentuk unit khusus bernama *Cyber Command* di bawah Kementerian Pertahanan Nasional, yang bertugas mengembangkan dan melaksanakan operasi siber, baik untuk tujuan pertahanan maupun untuk aksi ofensif terbatas dalam rangka penangkalan. Pendekatan ini mencerminkan penerapan *deterrence by punishment*, di mana negara memberikan sinyal bahwa serangan siber tidak akan dibiarkan tanpa konsekuensi. Meski terbatas dalam publikasi resmi, berbagai laporan intelijen internasional menunjukkan bahwa Korea Selatan memiliki kemampuan serangan balik siber terhadap sistem yang digunakan oleh kelompok proksi Korea Utara.

Korea Selatan memiliki badan sipil bernama *Korea Internet and Security Agency* (KISA) yang berperan dalam mengelola insiden siber, memberikan pelatihan, membangun kesadaran publik, serta melakukan investigasi digital terhadap aktivitas peretasan. KISA bekerja sama erat dengan sektor swasta dan lembaga publik lainnya dalam membangun *cyber resilience*, sebagai bentuk *deterrence by denial*. Upaya ini diperkuat dengan sistem deteksi dini dan peringatan cepat yang terus dikembangkan melalui teknologi berbasis kecerdasan buatan dan data besar.

Strategi Deterrence Siber Indonesia terhadap Ancaman Proxy State Actor

Indonesia menghadapi tantangan serius dalam membangun strategi deterrence siber yang efektif terhadap ancaman *proxy state actor*. Di tengah transformasi digital nasional yang pesat, kerentanan terhadap serangan siber juga meningkat, terutama dari aktor-aktor yang tidak secara langsung mewakili negara namun memiliki afiliasi dengan kepentingan negara asing. Sayangnya, pendekatan Indonesia dalam merespons ancaman ini masih lebih bersifat defensif, administratif, dan reaktif dibandingkan strategis dan terkoordinasi (Suwarno & Widodo, 2022).

Strategi utama yang saat ini dijalankan Indonesia mengacu pada penguatan kelembagaan melalui pembentukan Badan Siber dan Sandi Negara (BSSN) dan penerbitan Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital. Upaya ini menjadi fondasi untuk *deterrence by denial*, yaitu memperkuat sistem pertahanan agar serangan menjadi tidak efektif. Namun, dalam praktiknya, sistem keamanan nasional di Indonesia masih menghadapi berbagai kendala serius. Menurut Laporan Kajian Strategis Lemhannas (2021), kapasitas teknis lembaga pertahanan dan keamanan di tingkat daerah belum merata, terutama dalam hal infrastruktur pemantauan dan integrasi sistem informasi. Selain itu, data Kemenpan-RB tahun 2020 menunjukkan kekurangan signifikan dalam jumlah personel keamanan siber yang kompeten. Koordinasi antar lembaga seperti TNI, Polri, dan Badan Siber dan Sandi Negara (BSSN) juga dinilai belum optimal, sebagaimana dicatat dalam evaluasi Kementerian Koordinator Politik, Hukum, dan Keamanan (Kemenko Polhukam). Di sisi lain, partisipasi sektor privat, terutama dalam melindungi infrastruktur vital nasional seperti jaringan telekomunikasi dan energi, masih minim akibat kurangnya regulasi insentif dan kejelasan peran mereka dalam sistem keamanan nasional

Dalam hal *deterrence by punishment*, Indonesia belum memiliki perangkat yang cukup memadai untuk memberikan efek tangkal. Belum ada kebijakan yang memungkinkan respons aktif terhadap serangan, baik dalam bentuk sanksi ekonomi, tindakan hukum terhadap pelaku internasional, maupun kerja sama intelijen dalam rangka penegakan atribusi. Selain itu, mekanisme atribusi serangan masih belum kuat, yang menyebabkan kesulitan dalam menentukan pelaku serangan secara sah dan meyakinkan di ranah diplomatik maupun hukum internasional (Nefo et al., 2025).

Indonesia masih belum sepenuhnya aktif dalam diplomasi siber di tingkat regional dan global. Laporan dari CSIS Indonesia (2023) menyebutkan bahwa partisipasi Indonesia dalam perundingan siber internasional masih terbatas, baik dalam kerangka ASEAN maupun forum global seperti United Nations Open-ended Working Group (OEWG) on ICTs. Kerja sama dalam ASEAN Cybersecurity Cooperation Strategy serta peluang ratifikasi Budapest

Convention on Cybercrime belum dimanfaatkan secara optimal untuk memperkuat legitimasi kebijakan deterrence Indonesia. Menurut (Nefo et al., 2025) strategi deterrence Indonesia terhadap proxy state actor masih berada pada tahap konseptual, dengan keterbatasan dalam mekanisme atribusi dan respons. Untuk meningkatkan efektivitasnya, Indonesia perlu memperkuat teknologi atribusi digital, memperluas kerja sama internasional dengan negara mitra seperti Singapura dan Australia, serta mengembangkan kebijakan responsif berbasis kerangka cyber deterrence theory yang menekankan pada denial, punishment, dan resilience. Pendekatan ini penting agar pelaku serangan dan negara sponsor merasakan efek jera, serta untuk memperkuat posisi Indonesia dalam tatanan keamanan siber global.

Stefan Soesanto (2022) mengusulkan enam mekanisme utama dalam kerangka cyber deterrence: *deterrence by denial*, *deterrence by punishment*, *delegitimization*, *entanglement*, *reputation*, dan *cross-domain deterrence*. Dua di antaranya menjadi landasan utama dalam strategi nasional sebagian besar negara, yaitu denial dan punishment. *Deterrence by denial* menekankan pada peningkatan sistem pertahanan internal agar serangan menjadi sulit dilakukan atau tidak efektif. Ini mencakup proteksi sistem, redundansi jaringan, respons insiden yang cepat, dan peningkatan kapasitas sumber daya manusia. Sementara itu, *deterrence by punishment* melibatkan ancaman pembalasan, baik dalam bentuk serangan balik siber, sanksi ekonomi, atau tindakan diplomatik terhadap negara atau aktor yang terbukti melakukan serangan (Wibowo et al., 2024).

Negara-negara seperti Singapura dan Korea Selatan telah mengembangkan strategi cyber deterrence yang relatif komprehensif. Singapura mengandalkan pendekatan defensif berbasis *denial* melalui penguatan sistem nasional, pelatihan keamanan siber, dan kebijakan hukum seperti *Cybersecurity Act 2018*. Korea Selatan, dengan ancaman langsung dari Korea Utara, menerapkan strategi kombinasi antara denial dan punishment dengan membentuk unit militer siber dan meningkatkan kerja sama intelijen internasional. Indonesia saat ini masih dalam proses membangun kerangka cyber deterrence nasional. Meski telah terbentuk BSSN dan ada kebijakan perlindungan infrastruktur informasi vital, implementasinya masih menghadapi berbagai kendala, mulai dari koordinasi antarinstansi hingga keterbatasan SDM dan teknologi. Cyber deterrence belum dijadikan pilar utama dalam strategi pertahanan nasional, dan diplomasi siber Indonesia pun masih bersifat pasif.

Dampak Ekonomi

Teori *cyber deterrence* menjelaskan bahwa pencegahan terhadap serangan siber dapat dibangun melalui beberapa mekanisme seperti *deterrence by denial*, *deterrence by punishment*,

delegitimization, serta *entanglement* dan *reputation*. Dalam konteks Indonesia, keempat mekanisme ini belum sepenuhnya terimplementasi secara efektif. Salah satu bukti nyata lemahnya daya tangkal siber Indonesia adalah kasus serangan ransomware terhadap Pusat Data Nasional (PDN) pada Juni 2024. Serangan tersebut mengenkripsi sistem layanan milik lebih dari 200 institusi pemerintah, termasuk layanan imigrasi, bandara, hingga kependudukan. Kelumpuhan layanan digital berskala nasional ini menunjukkan bahwa strategi *deterrence by denial* Indonesia masih sangat lemah, terutama dari sisi backup, mitigasi, dan respons insiden.

Audit BPK menunjukkan bahwa 98% data di PDN bahkan tidak memiliki backup, yang memperparah dampak serangan. Selain mengganggu layanan publik, serangan ini menimbulkan kerugian ekonomi yang sangat besar. Menurut perhitungan Celios, kerugian akibat serangan PDN mencapai Rp6,3 triliun, termasuk biaya pemulihan, downtime, serta dampak tidak langsung seperti hilangnya kepercayaan publik dan terhambatnya produktivitas layanan vital. Sementara itu, dari sisi *deterrence by punishment*, Indonesia belum memiliki kapabilitas atribusi yang cukup untuk mengidentifikasi pelaku secara akurat dan menindak tegas, baik melalui jalur hukum, diplomatik, maupun ofensif.

Mekanisme *delegitimization* pun belum berjalan karena Indonesia belum aktif mendorong norma atau penegakan hukum internasional terhadap aktor siber. Rendahnya reputasi dan kurangnya keterlibatan dalam kerja sama keamanan siber internasional membuat Indonesia tidak cukup ‘menakutkan’ bagi pelaku. Oleh karena itu, lemahnya implementasi *cyber deterrence* Indonesia tidak hanya berisiko terhadap keamanan digital, tetapi juga mengancam stabilitas ekonomi nasional secara langsung.

Analisis Komparatif

Tabel 1. Analisis Komparatif

No.	Tolak Ukur Strategi Deterrence Siber	Korea Selatan	Singapura	Indonesia
1	**Kemampuan atribusi yang valid**	Sangat kuat. Memiliki unit *cyber command* militer dan forensik digital tingkat lanjut yang mampu mengidentifikasi pelaku, terutama terkait ancaman dari Korea Utara.	Cukup kuat. Mengandalkan CSA dan kerja sama internasional dalam threat intelligence untuk memperkuat atribusi.	Lemah. Belum ada mekanisme atribusi nasional yang efektif; kesulitan mengidentifikasi pelaku serangan besar seperti pada kasus PDN 2024.

No.	Tolak Ukur Strategi Deterrence Siber	Korea Selatan	Singapura	Indonesia
2	**Kapabilitas teknis dalam deteksi, analisis, dan pemulihan serangan**	Tinggi. Sistem deteksi dini, AI-based monitoring, dan pemulihan terintegrasi antara militer dan sipil.	Tinggi. Sistem audit dan uji keamanan reguler, sertifikasi perangkat, serta tim respons insiden aktif.	Rendah. Kasus PDN 2024 menunjukkan minimnya backup data dan keterlambatan pemulihan; 98% data tidak dibackup.
3	**Koherensi kebijakan antara lembaga sipil dan militer**	Sangat terkoordinasi. Ada integrasi langsung antara Kementerian Pertahanan, KISA (sipil), dan satuan militer.	Koordinatif. CSA sebagai lembaga sipil memiliki otoritas lintas sektor dan didukung penuh oleh pemerintah pusat.	Kurang. BSSN belum mampu mengoordinasikan semua sektor; kebijakan masih tersebar dan sektoral.
4	**Respon diplomatik dan hukum yang konsisten**	Aktif. Secara diplomatik tegas terhadap ancaman dari Korea Utara, termasuk kampanye internasional.	Proaktif. Terlibat dalam forum internasional dan memiliki regulasi kuat (Cybersecurity Act 2018).	Pasif. Minim keterlibatan dalam diplomasi siber global; belum ada UU khusus keamanan siber, hanya Perpres teknis.

Tabel di atas menggambarkan perbandingan strategi *cyber deterrence* ketiga negara berdasarkan empat indikator utama. Korea Selatan menunjukkan performa paling kuat, terutama dalam kemampuan atribusi dan koordinasi antara lembaga militer dan sipil. Negara ini memiliki *cyber command* aktif yang memungkinkan respons cepat terhadap ancaman, khususnya dari Korea Utara. Dari sisi teknis, Korea Selatan juga unggul dengan sistem deteksi berbasis kecerdasan buatan dan strategi pemulihan yang komprehensif. Singapura menempati posisi kedua, dengan pendekatan defensif berbasis lembaga sipil, yaitu Cyber Security Agency (CSA), yang memiliki kewenangan lintas sektor. Singapura unggul dalam regulasi, deteksi insiden, serta respons diplomatik melalui forum internasional.

Indonesia masih menunjukkan kelemahan di semua indikator. Kasus serangan ransomware terhadap Pusat Data Nasional pada 2024 mengindikasikan lemahnya atribusi, kapasitas teknis, dan ketiadaan sistem pemulihan yang layak. Koordinasi antarlembaga masih bersifat sektoral, dan belum ada kerangka hukum nasional khusus terkait keamanan siber. Ketiadaan peran aktif dalam diplomasi siber global juga memperlemah posisi Indonesia dalam menanggapi ancaman dari aktor siber asing. Hal ini menunjukkan perlunya perbaikan mendasar dalam strategi keamanan siber Indonesia.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa strategi deterrence siber Indonesia terhadap ancaman proxy state actor masih belum efektif secara optimal. Meskipun telah memiliki institusi seperti BSSN dan kebijakan dasar seperti Perpres No. 82 Tahun 2022, Indonesia masih tertinggal dalam aspek atribusi, penegakan hukum, dan kerja sama internasional yang diperlukan untuk membangun efek penangkalan yang kredibel. Berbeda dengan Singapura yang menonjol dalam strategi deterrence by denial melalui penguatan sistem dan regulasi, serta Korea Selatan yang menggabungkan pendekatan denial dan punishment melalui integrasi militer-sipil dan kapabilitas ofensif terbatas, Indonesia masih berada pada tahap penguatan struktur kelembagaan dan pengembangan kapasitas. Penelitian ini menunjukkan bahwa efektivitas deterrence sangat dipengaruhi oleh kejelasan otoritas, integrasi kebijakan lintas sektor, kemampuan atribusi, dan legitimasi hukum serta diplomatik. Diperlukan reformasi menyeluruh terhadap pendekatan keamanan siber Indonesia, termasuk penyusunan undang-undang keamanan siber nasional, peningkatan kompetensi sumber daya manusia, serta perluasan kerja sama internasional, baik secara bilateral maupun multilateral. Peneliti menyadari bahwa penelitian ini memiliki keterbatasan, terutama karena bersifat kualitatif dan tidak melibatkan data primer dari pihak pembuat kebijakan secara langsung. Penelitian lanjutan dengan pendekatan studi kasus lapangan atau metode kuantitatif sangat disarankan guna memperkuat validitas temuan dan memberikan kontribusi yang lebih aplikatif dalam perumusan strategi keamanan siber Indonesia ke depan.

DAFTAR REFERENSI

Bhakti, A., Sudirman, A., Widya Setiabudi Sumadinata, R., & Bainus, A. (2024). State defense strategy in facing cyber threats after hacking incidents on government institutions: A case study in Indonesia. Journal of Human Security, 20(1), 109–117. https://doi.org/10.12924/johs2024.20116

Darumaya, B. A., Maarif, S., Toruan, T., Swastanto, Y., Doktoral, P., & Strategi, F. (2023). Pemikiran potensial ancaman perang siber di Indonesia: Suatu kajian strategi pertahanan. Jurnal Pertahanan, IX(2), 299–324.

Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global, 7(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Heryadi, D., Rizaldi, R., Rahmadhani, T. P., Miranti, F. D., Juliastica, F., & Info, A. (2024). Indonesia's role as a cyber protector in the Southeast Asia region. Nasionalism dan Integrity, 10(1), 169–187. https://doi.org/10.33172/jp

Ma'aliya, N., Adriyanto, A., Prasetyo, T. B., & Sutanto, R. (2023). Analysis of hybrid warfare threat perception on Indonesian national defense. International Journal of Progressive Sciences and Technologies (IJPSAT), 37(1), 732–740.

Nefo, S., Kertopati, H., & Studi, P. (2025). Perspektif intelijen sosial budaya: Kewarganegaraan dan bela negara dalam masyarakat majemuk Indonesia. Jurnal Kewarganegaraan, 4(1), 1029.

Ramadhan, G. (2025). Analisis strategi keamanan nasional Indonesia dalam menghadapi ancaman siber. Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi, 2(2).

Subrata, A. A., Tobing, C., Staf, S., Komando, D., & Laut, A. (n.d.). Analisis perang Rusia-Ukraina tahun 2022 menggunakan metode PESTLE serta manfaatnya bagi TNI Angkatan Laut. https://doi.org/10.52307/jmi

Suwarno, P., & Widodo, P. (2022). Strategi pemerintah dalam menghadapi proxy war sebagai salah satu penyebab gerakan separatisme di Indonesia. Jurnal Kewarganegaraan, 6(2).

Vimy, T., Wiranto, S., Widodo, P., Suwarno, P., Studi Keamanan Maritim, P., Keamanan Nasional, F., & Pertahanan Republik Indonesia, U. (2022). Ancaman serangan siber pada keamanan nasional Indonesia. Jurnal Kewarganegaraan, 6(1).

Wibowo, S. E., Hartono, A., Kiswanto, H., Primawanti, H., Torang, J., & Louerens, A. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. Global Political Studies Journal, 8. https://doi.org/10.34010/gpsjournal.v8i2