Jurnal Cendekia Hukum Indonesia
Vol. 2 No. 2 Oktober 2026
Licenced CC BY-SA, E-ISSN: 3090-6229, Hal 118-130
DOI: https://doi.org/10.71417/jchi.v2i2.225.
https://hukum.journalpustakacendekia.com/index.php/JCHI

Kesiapan Kebijakan Keamanan Siber Indonesia terhadap Ancaman Serangan Stuxnet : Pembelajaran dari Kasus Iran

Adam Muhammad Ridwan[1*], Miftahul Ulum[2]

[12]Ilmu Politik, Universitas Muhammadiyah Jakarta, Indonesia

Alamat: Jl. K.H. Ahmad Dahlan, Cirendeu, Ciputat, Tangerang Selatan, Banten
E-mail: adammuhammadridwan123@gmail.com,miftahul.ulum@umj.ac.id

Abstract: *The advancement of digital transformation and increasing reliance on technology-based infrastructure have made cybersecurity a strategic issue in national security. The Stuxnet attack in 2010 served as a significant milestone, demonstrating that cyber threats are capable of causing physical damage to a nation's critical infrastructure. As one of the countries with the highest rates of Stuxnet infection, Indonesia faces serious challenges in strengthening its national cybersecurity resilience. This study aims to analyze the readiness of Indonesia's cybersecurity policies in addressing strategic threats such as Stuxnet by drawing lessons from Iran's post-attack cybersecurity transformation. The study employs a qualitative approach using a comparative study method through the analysis of policy documents, regulations, scientific journals, and academic literature related to cybersecurity in Indonesia and Iran. Data analysis was conducted using content analysis grounded in the theory of cybersecurity politics. The research findings indicate that Indonesia still faces challenges related to institutional fragmentation, limited human resources, and weak cross-sectoral coordination in cybersecurity management. In contrast, Iran has been able to undergo rapid transformation through a centralized command model that strengthens national cybersecurity capabilities, although this has led to increased militarization and restrictions on civil liberties. This study concludes that Indonesia needs to strengthen cybersecurity governance, institutional integration, human resource development, and national cybersecurity resilience strategies without neglecting the principles of democracy, the rule of law, and human rights.*

Keywords: *Cybersecurity, Security Policy, Stuxnet*

Abstrak: Perkembangan transformasi digital dan meningkatnya ketergantungan terhadap infrastruktur berbasis teknologi telah menjadikan keamanan siber sebagai isu strategis dalam keamanan nasional. Serangan Stuxnet pada tahun 2010 menjadi tonggak penting yang menunjukkan bahwa ancaman siber mampu menimbulkan kerusakan fisik terhadap infrastruktur kritis suatu negara. Indonesia sebagai salah satu negara dengan tingkat infeksi Stuxnet tertinggi menghadapi tantangan serius dalam memperkuat ketahanan keamanan siber nasional. Penelitian ini bertujuan untuk menganalisis kesiapan kebijakan keamanan siber Indonesia dalam menghadapi ancaman strategis seperti Stuxnet dengan mengambil pembelajaran dari transformasi keamanan siber Iran pasca-serangan tersebut. Penelitian menggunakan pendekatan kualitatif dengan metode studi komparatif melalui analisis dokumen kebijakan, regulasi, jurnal ilmiah, dan literatur akademik terkait keamanan siber Indonesia dan Iran. Teknik analisis data dilakukan menggunakan content analysis berbasis teori politik keamanan siber. Hasil penelitian menunjukkan bahwa Indonesia masih menghadapi permasalahan fragmentasi kelembagaan, keterbatasan sumber daya manusia, serta lemahnya koordinasi lintas sektor dalam pengelolaan keamanan siber. Sebaliknya, Iran mampu melakukan transformasi cepat melalui model komando terpusat yang memperkuat kapasitas keamanan siber nasional, meskipun berdampak pada meningkatnya militerisasi dan pembatasan kebebasan sipil. Penelitian ini menyimpulkan bahwa Indonesia perlu memperkuat tata kelola keamanan siber, integrasi kelembagaan, pengembangan SDM, serta strategi ketahanan siber nasional tanpa mengabaikan prinsip demokrasi, hukum, dan hak asasi manusia.

Kata Kunci: Keamanan Siber, Kebijakan Keamanan, Stuxnet

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital secara masif dalam berbagai sektor kehidupan, termasuk pemerintahan, industri, pertahanan, dan layanan publik. Integrasi sistem digital dengan Cyber-Physical Systems (CPS) menjadikan infrastruktur modern

Received: May 29, 2026; Revised: May 31, 2026; Accepted: June 04, 2026;
*Adam Muhammad Ridwan, adammuhammadridwan123@gmail.com

semakin efisien, namun di sisi lain meningkatkan ketergantungan terhadap ruang siber sebagai domain strategis keamanan nasional. Infrastruktur kritis seperti energi, transportasi, telekomunikasi, dan layanan keuangan kini rentan terhadap ancaman siber yang dapat menimbulkan gangguan operasional berskala besar dan berdampak pada stabilitas ekonomi maupun politik suatu negara. Menurut United Nations Office for Disarmament Affairs, ancaman siber terhadap infrastruktur kritis telah berkembang menjadi isu keamanan internasional yang membutuhkan tata kelola dan strategi pertahanan negara yang terintegrasi. Kondisi ini menunjukkan bahwa keamanan siber tidak lagi dipandang hanya sebagai isu teknis, melainkan telah menjadi bagian dari strategi geopolitik dan keamanan nasional modern (Rid, 2022.

Fenomena perubahan ancaman siber secara global mulai terlihat jelas sejak terungkapnya serangan Stuxnet pada tahun 2010. Malware ini menjadi tonggak sejarah karena merupakan senjata siber pertama yang mampu menimbulkan kerusakan fisik terhadap sistem industri melalui eksploitasi Industrial Control Systems (ICS). Stuxnet menyerang fasilitas nuklir Natanz di Iran dengan merusak lebih dari 1.000 sentrifuga dan memperlambat program nuklir Iran selama lebih dari satu tahun. Serangan ini menunjukkan bahwa ruang siber dapat digunakan sebagai instrumen perang strategis tanpa melibatkan konfrontasi militer konvensional secara langsung. Selain berdampak pada sektor teknis, Stuxnet juga memicu perubahan paradigma global mengenai keamanan siber, terutama dalam perlindungan infrastruktur kritis nasional dan pengembangan kebijakan pertahanan siber negara (Loukas, 2015; Kenney, 2015; Raja et al., 2025). Pasca-Stuxnet, berbagai serangan terhadap infrastruktur strategis terus meningkat, termasuk serangan terhadap jaringan listrik Ukraina yang memperlihatkan bagaimana ancaman siber dapat melumpuhkan layanan publik dan memicu ketidakstabilan nasional (Sen et al., 2022; Zhen & Gao, 2023).

Urgensi penelitian mengenai keamanan siber semakin relevan dalam konteks Indonesia yang tengah mengalami percepatan transformasi digital dan implementasi Internet of Things (IoT) pada berbagai sektor strategis. Tingginya ketergantungan terhadap sistem digital menyebabkan meningkatnya permukaan serangan (attack surface) dan potensi eksploitasi terhadap infrastruktur nasional. Fakta bahwa Indonesia pernah menjadi negara dengan tingkat infeksi Stuxnet tertinggi kedua di dunia setelah Iran menunjukkan bahwa Indonesia memiliki kerentanan nyata terhadap ancaman siber global (Shakarian, 2013). Selain itu, berbagai kasus kebocoran data dan gangguan sistem digital dalam beberapa tahun terakhir mengindikasikan bahwa ketahanan keamanan siber nasional masih menghadapi tantangan serius. Pemerintah melalui Badan Siber dan Sandi Negara telah berupaya memperkuat tata kelola keamanan siber melalui pembentukan strategi nasional dan peningkatan koordinasi keamanan digital. Namun demikian, berbagai penelitian menunjukkan bahwa implementasi kebijakan keamanan siber di Indonesia masih menghadapi kendala dalam aspek regulasi, koordinasi lintas sektor, penguatan kapasitas sumber daya manusia, serta perlindungan infrastruktur kritis nasional (Hossain et al., 2025; Abdillah et al., 2024). Oleh karena itu, penguatan ketahanan siber nasional menjadi kebutuhan mendesak guna menghadapi ancaman siber strategis yang semakin kompleks dan transnasional.

Kesenjangan penelitian (research gap) dalam kajian ini terletak pada masih terbatasnya studi komparatif yang secara khusus menganalisis kesiapan keamanan siber Indonesia dengan mempelajari transformasi dan respons Iran pasca-serangan Stuxnet. Penelitian terdahulu umumnya berfokus pada aspek teknis serangan siber, tata kelola keamanan siber nasional, maupun strategi perlindungan infrastruktur kritis secara umum, tetapi belum mengkaji secara mendalam perbandingan kebijakan, model tata kelola, dan strategi ketahanan siber antara Indonesia dan Iran sebagai dua negara yang sama-sama terdampak oleh penyebaran Stuxnet. Literatur yang tersedia juga menunjukkan bahwa kajian keamanan siber Indonesia masih relatif terbatas dalam publikasi internasional dan belum banyak mengangkat pembelajaran strategis dari negara lain yang mengalami transformasi keamanan siber akibat ancaman siber-fisik (Hossain et al., 2025; Wahyudi et al., 2025). Padahal, analisis komparatif tersebut penting untuk memahami bagaimana suatu negara membangun kapasitas keamanan siber,

mengembangkan strategi pertahanan digital, dan memperkuat perlindungan infrastruktur kritis dalam menghadapi ancaman siber tingkat tinggi. Dengan demikian, penelitian ini diharapkan mampu mengisi kekosongan kajian akademik sekaligus memberikan kontribusi praktis bagi penguatan kebijakan keamanan siber nasional Indonesia.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi komparatif (comparative case study) untuk menganalisis politik keamanan siber Indonesia dan Iran pasca-serangan Stuxnet. Pendekatan kualitatif dipilih karena mampu mengeksplorasi secara mendalam dinamika sosial, politik, dan kebijakan yang melatarbelakangi penguatan keamanan siber di kedua negara. Melalui metode studi komparatif, penelitian ini berupaya mengidentifikasi persamaan, perbedaan, serta pola respons kebijakan keamanan siber antara Indonesia dan Iran dalam menghadapi ancaman siber strategis. Penelitian dilaksanakan pada rentang waktu 2025–2026 dengan fokus kajian pada konteks kebijakan keamanan siber di Indonesia dan Iran. Penelitian ini tidak dilakukan pada lokasi geografis tertentu, melainkan pada ruang analitis berupa dokumen kebijakan, regulasi, dan literatur akademik yang berkaitan dengan keamanan siber kedua negara. Analisis Indonesia difokuskan pada perkembangan kebijakan pasca-pembentukan Badan Siber dan Sandi Negara tahun 2017 hingga periode terkini, sedangkan analisis Iran difokuskan pada transformasi kebijakan pasca-serangan Stuxnet tahun 2010 hingga perkembangan keamanan siber mutakhir.

Sumber data penelitian ini menggunakan data sekunder yang berasal dari dokumen kebijakan resmi, regulasi pemerintah, jurnal ilmiah, buku akademik, laporan lembaga internasional, serta publikasi institusi terkait keamanan siber. Data dikumpulkan melalui teknik studi dokumentasi dan studi pustaka dengan menelaah berbagai sumber yang relevan mengenai politik keamanan siber Indonesia dan Iran. Dokumen yang dianalisis meliputi strategi keamanan siber nasional, regulasi perlindungan data, laporan lembaga keamanan siber, serta kajian akademik mengenai Stuxnet dan ketahanan siber nasional. Teknik analisis data yang digunakan adalah analisis isi (content analysis) dengan pendekatan terpandu teori (theory-guided content analysis). Proses analisis dilakukan melalui tahap pengkodean, kategorisasi, analisis tematik, dan interpretasi berdasarkan kerangka Politik Keamanan Siber yang mencakup aspek aktor, proses, kepentingan, dan konteks kebijakan. Selain itu, penelitian ini juga menggunakan analisis komparatif sistematis untuk membandingkan respons kebijakan kedua negara serta analisis naratif untuk merekonstruksi transformasi keamanan siber pasca-Stuxnet. Validitas data diperkuat melalui teknik triangulasi sumber dengan membandingkan berbagai dokumen akademik, kebijakan, dan laporan institusional agar diperoleh hasil penelitian yang mendalam dan objektif.

3. HASIL DAN PEMBAHASAN

Pengaturan dan Perlindungan Hukum Tindak Pidana Revenge Berdasarkan Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Penelitian ini menemukan bahwa dinamika politik keamanan siber Indonesia dan Iran menunjukkan perbedaan signifikan dalam merespons ancaman siber strategis pasca-peristiwa Stuxnet. Iran melakukan sekuritisasi tinggi terhadap ancaman siber dan meresponsnya melalui restrukturisasi

kelembagaan yang terpusat serta penguatan postur keamanan yang defensif-keras. Sebaliknya, Indonesia mengembangkan kebijakan keamanan siber secara gradual melalui pendekatan tata kelola dan regulasi, dengan tingkat sekuritisasi yang lebih moderat sebagaimana tercermin dalam penyusunan strategi nasional dan penguatan kelembagaan secara bertahap.

Temuan penelitian juga menunjukkan bahwa meskipun Indonesia tidak menjadi target sabotase fisik dalam kasus Stuxnet, tingginya tingkat infeksi malware pada fase awal penyebaran—sekitar 15.000 sistem mengindikasikan eksposur signifikan terhadap infiltrasi siber canggih. Angka tersebut merujuk pada sistem yang terinfeksi sebagai media penyebaran, bukan sebagai target sabotase industri strategis. Perbedaan pengalaman krisis ini memengaruhi konfigurasi aktor, proses kebijakan, serta pembentukan postur keamanan siber kedua negara. Secara keseluruhan, hasil penelitian menegaskan bahwa intensitas sekuritisasi, struktur kelembagaan, dan konteks geopolitik menjadi faktor penentu dalam pembentukan politik keamanan siber suatu negara (Ulum, 2026)

Evolusi Ancaman Stuxnet dan Implikasinya terhadap Keamanan Nasional

Perkembangan ancaman siber strategis global tidak dapat dilepaskan dari peristiwa Stuxnet pada tahun 2010 yang menandai transformasi fundamental dalam lanskap keamanan internasional. Serangan tersebut menunjukkan bahwa ruang siber dapat digunakan sebagai instrumen strategis untuk menghasilkan dampak fisik terhadap infrastruktur kritis suatu negara tanpa konfrontasi militer terbuka. Pasca-peristiwa tersebut, ancaman siber berkembang menjadi pola serangan yang semakin presisi, terarah, dan sulit diatribusikan.

Indonesia sendiri tercatat sebagai salah satu negara dengan tingkat deteksi infeksi Stuxnet tertinggi kedua secara global pada fase awal penyebarannya, dengan estimasi sekitar 15.000 sistem terinfeksi. Meskipun tidak terdapat bukti bahwa infrastruktur kritis Indonesia mengalami sabotase fisik, fakta tersebut menunjukkan eksposur signifikan terhadap infiltrasi malware canggih. Dalam konteks transformasi digital nasional, pola ancaman *Stuxnet-like* tetap relevan sebagai kemungkinan risiko terhadap sistem industri dan sektor strategis. Sebagai ilustrasi konseptual, apabila serangan dengan karakteristik serupa terjadi pada sektor energi atau infrastruktur vital Indonesia, dampaknya tidak hanya bersifat teknis, tetapi juga berpotensi memengaruhi stabilitas ekonomi, legitimasi politik, serta kepercayaan publik terhadap kapasitas negara dalam menjaga keamanan nasional. Oleh karena itu, pembahasan hasil penelitian pada bab ini ditempatkan dalam konteks evolusi ancaman siber strategis tersebut.

Konstelasi Aktor dan Kelembagaan

Landskap kelembagaan keamanan siber Indonesia merupakan cerminan dari kompleksitas sistem politiknya yang desentralistik, serta dialektika permanen antara kepentingan keamanan nasional, pertumbuhan ekonomi digital, dan hak-hak sipil. Analisis terhadap konstelasi aktor mengungkap sebuah arsitektur tata kelola yang multi-lembaga, terfragmentasi, dan belum sepenuhnya terintegrasi. Meskipun Badan Siber dan Sandi Negara (BSSN) secara formal ditetapkan sebagai koordinator nasional, dinamika operasional justru didominasi oleh tumpang tindih kewenangan (overlap), kompetisi sumber daya, dan kesenjangan koordinasi yang signifikan, sehingga membentuk postur defensif yang cenderung reaktif dalam menghadapi ancaman strategis (Mulyadi & Rahayu, 2019; Priyandita & Lebang, 2025).

Pemetaan Aktor Kunci: Fragmentasi antara Koordinasi, Regulasi, dan Pertahanan

Peta kekuasaan dalam ranah siber Indonesia diisi oleh aktor-aktor dengan persepsi ancaman, kepentingan, dan sumber daya yang berbeda-beda, yang sering kali tidak selaras.

1. Badan Siber dan Sandi Negara (BSSN): Koordinator dengan Wewenang yang Teruji
   Didirikan pada tahun 2017 melalui Perpres No. 53, BSSN merupakan transformasi dari Lembaga Sandi Negara (Lemsaneg). Secara hukum, BSSN ditugaskan sebagai otoritas koordinatif utama dengan tiga pilar tugas: pertahanan siber, keamanan siber, dan sandi negara. Mandatnya mencakup penyusunan kebijakan nasional, perlindungan Infrastruktur Informasi Kritis Nasional (IIKN), dan operasionalisasi *Gov-CSIRT* sebagai ujung tombak penanganan insiden (Mulyadi & Rahayu, 2019).

Namun, posisinya sebagai "koordinator" tanpa kewenangan hierarkis yang kuat atas kementerian teknis dan lembaga keamanan menjadi tantangan struktural. Kapasitasnya sering kali diuji oleh institusi lain yang memiliki garis anggaran, personel, dan mandat operasional yang lebih mapan dan independen, sehingga koordinasi lebih banyak bergantung pada persuasi dan kolaborasi sukarela yang tidak selalu efektif dalam situasi krisis.

2. Kementerian Komunikasi dan Informatika (Kemenkominfo): Regulator Ekosistem Digital Sebagai regulator utama ruang digital Indonesia, Kemenkominfo memegang kendali atas aspek-aspek fundamental seperti perizinan spektrum frekuensi, registrasi nama domain (*.id*), dan penetapan standar teknis untuk penyelenggara sistem elektronik. Kewenangan luas ini menciptakan area tumpang tindih kebijakan dengan BSSN, terutama dalam menetapkan standar keamanan dan ketahanan untuk platform digital, e-commerce, dan layanan cloud. Misalnya, insiden kebocoran data masif dari sebuah platform digital dapat memicu respons paralel dari BSSN (sebagai insiden keamanan siber) dan Kemenkominfo (sebagai pelanggaran terhadap Peraturan Menteri tentang Perlindungan Data Pribadi). Dinamika ini menunjukkan belum adanya pembagian peran (*role delineation*) yang jelas dan protokol tunggal untuk insiden semacam itu.
3. Aktor Keamanan dan Pertahanan (TNI & Polri): Dikotomi antara *Cybercrime* dan *Cyber Warfare* Fragmentasi paling krusial dan berpotensi disfungsional terjadi pada pemisahan tajam antara domain keamanan dalam negeri (*cybersecurity*) dan pertahanan kedaulatan (*cyber defence*).
4. Kepolisian Republik Indonesia (Polri), melalui Direktorat Tindak Pidana Siber Bareskrim, mendefinisikan ancaman siber terutama sebagai kejahatan konvensional yang menggunakan medium digital (*cybercrime*). Fokusnya adalah pada penegakan hukum terhadap aktivitas seperti penipuan online, pemerasan siber (*ransomware*), ujaran kebencian, dan penyebaran konten terlarang. Pendekatannya bersifat reaktif-investigatif dan berorientasi pada pembuktian di pengadilan (Anwary, 2022).
5. Tentara Nasional Indonesia (TNI), melalui Pusat Siber TNI yang berada di bawah Kementerian Pertahanan, membangun kerangka ancaman yang sangat berbeda. Ancaman dipersepsikan sebagai serangan yang bermotif politik-militer dari aktor negara lain atau kelompok yang didukung negara, yang bertujuan untuk melumpuhkan infrastruktur strategis, mencuri rahasia intelejen, atau mengganggu stabilitas nasional. Kapabilitas yang dibangun, meski masih dalam tahap pengembangan, berorientasi pada pertahanan aset militer dan negara serta deterensi dalam ranah siber (Bhakti et al., 2024; Priyandita & Lebang, 2025).

Implikasi dari dikotomi ini adalah "zona abu-abu" yang berbahaya. Serangan siber canggih seperti *Distributed Denial-of-Service* (DDoS) terhadap bursa saham atau infiltrasi bertahap (*advanced persistent threat*) ke jaringan perusahaan energi milik negara bisa jadi tidak memenuhi kriteria "kejahatan" yang jelas untuk Polri, tetapi juga belum dikategorikan sebagai "serangan militer" yang memicu respons TNI. Absennya kerangka komando gabungan (*joint task force*) dan kriteria eskalasi yang baku untuk insiden-insiden *hybrid* semacam ini berpotensi menyebabkan kelambanan respons (*response lag*) atau tanggapan yang terfragmentasi.

Keterlibatan Non-State Actor: Kemitraan yang Masih Formalistis

Di luar struktur pemerintah, partisipasi sektor swasta—khususnya operator IIKN di bidang energi, keuangan, dan telekomunikasi—sangat penting namun dihadapkan pada hambatan struktural (Saputra et al., 2019). Meskipun konsep Kemitraan Publik-Swasta (PPP) secara resmi diakui, implementasinya seringkali belum melampaui forum dialog dan pelatihan bersama. Kurangnya perjanjian formal yang mengikat mengenai berbagi intelijen ancaman secara real-time, audit keamanan bersama, dan kerangka respons insiden terpadu menjadi penghalang utama (Ponnusamy et al., 2019). Swasta enggan berbagi informasi detail karena kekhawatiran akan sanksi regulator dan dampak reputasi, sementara pemerintah belum memberikan insentif hukum yang cukup. Perbandingan dengan

negara seperti Jerman menunjukkan Indonesia masih tertinggal dalam membangun kerangka hukum yang mendukung pertukaran informasi ancaman yang aman dan terlindungi (Susila & Salim, 2024).

Sementara itu, peran komunitas akademik dan riset dalam menyediakan talenta, penelitian dasar, dan analisis kebijakan kritis juga belum terintegrasi secara optimal dalam kerangka tata kelola nasional. Keterlibatan mereka cenderung ad-hoc dan proyek-based, yang merupakan salah satu manifestasi dari pendekatan keamanan yang masih sangat state-centric dan kurang memanfaatkan kapasitas inovasi dari ekosistem sipil yang lebih luas (Priyandita & Lebang, 2025).

Proses Formulasi dan Implementasi Kebijakan

Proses politik di balik formulasi dan implementasi kebijakan keamanan siber Indonesia mencerminkan tarik-menarik antara logika perencanaan strategis jangka panjang dan tekanan untuk bereaksi terhadap insiden krisis yang terjadi. Analisis terhadap dokumen kebijakan utama dan pola respons insiden mengungkap bahwa meskipun kerangka strategis telah diletakkan, implementasi operasionalnya masih terhambat oleh kapasitas birokrasi, anggaran, dan paradigma keamanan yang belum sepenuhnya terinternalisasi (Priyandita & Lebang, 2025).

Respons Terhadap Ancaman: Antara Perencanaan dan Reaktivitas

Pasca-insiden siber besar, pola respons kebijakan Indonesia menunjukkan karakter yang reaktif dan ad-hoc. Siklus Politik Pasca-Krisis: Insiden besar seperti peretasan terhadap lembaga pemerintah sering kali memicu peringatan politik tinggi, yang mendorong respons langsung tetapi insidentil. Pola ini menunjukkan bahwa ancaman siber kerap dikelola sebagai krisis episodik yang memerlukan tanggapan administratif langsung, bukan sebagai risiko strategis berkelanjutan yang terintegrasi dalam perencanaan reguler (Bhakti et al., 2024). Hal ini mencerminkan kelemahan dalam kerangka regulasi yang ada untuk secara proaktif mencegah dan mengelola insiden siber (Anwary, 2022).

Kontras dengan Perencanaan Strategis: Di sisi lain, Indonesia telah memiliki dokumen perencanaan strategis sejak sebelum dan sesudah pembentukan BSSN (Mulyadi & Rahayu, 2019). Namun, terdapat kesenjangan (*gap*) yang lebar antara visi dalam dokumen-dokumen tersebut dengan program kerja, alokasi anggaran spesifik, dan pedoman operasional di tingkat kementerian teknis dan daerah. Akibatnya, perencanaan strategis sering kali tidak secara efektif mengarahkan keputusan alokasi sumber daya dan prioritas harian birokrasi (Priyandita & Lebang, 2025).

Sekuritisasi Ancaman Strategis Siber-Fisik: Wacana versus Internalisasi

Proses sekuritisasi—pembingkaian ancaman siber-fisik sebagai isu keamanan nasional yang mendesak—di Indonesia berjalan tidak merata dan belum mendalam. Dalam Wacana Kebijakan Resmi: Ancaman terhadap infrastruktur kritis akibat serangan siber telah diangkat dalam wacana kebijakan. Namun, penyebutannya dalam dokumen perencanaan masih umum dan tidak selalu disertai dengan skenario ancaman yang detail atau peta jalan teknis untuk mitigasi. Dengan kata lain, ancaman tersebut telah diakui (*recognized*) tetapi belum sepenuhnya tersekuritisasi (*securitized*) dalam arti memobilisasi sumber daya dan perubahan kebijakan yang luar biasa (Bhakti et al., 2024).

Hambatan Internalisasi: Hambatan utama adalah kompleksitas teknis dan distribusi tanggung jawab. Bagi banyak pembuat kebijakan di sektor fisik, risiko siber terhadap sistem kontrol industri merupakan konsep yang abstrak. Selain itu, karena infrastruktur kritis banyak dikelola BUMN dan swasta, negara menghadapi tantangan dalam menerapkan standar keamanan wajib secara efektif tanpa kerangka kemitraan yang kuat (Saputra et al., 2019; Ponnusamy et al., 2019).

Hambatan Implementasi: Dari Strategi ke Aksi di Tingkat Sektoral dan Daerah

Tantangan terberat terletak pada tahap implementasi, di mana strategi nasional harus diterjemahkan menjadi aksi konkret.

1. Kendala Anggaran dan SDM: Alokasi anggaran untuk keamanan siber di banyak instansi masih terbatas dan bersifat proyek-proyek lepasan. Keterbatasan SDM siber yang kompeten di dalam birokrasi juga parah, yang berdampak pada kapasitas untuk mengantisipasi dan menangkal ancaman secara efektif (Anwary, 2022).

2. Tantangan Koordinasi dan Kerangka Operasional: Implementasi inisiatif seperti Gov-CSIRT menghadapi tantangan dalam menjaga koordinasi dan efektivitasnya di masa depan, yang berkaitan dengan kurangnya kerangka operasional yang detail dan berkelanjutan (Wilis & Sidabutar, 2024). Tantangan serupa terlihat dalam upaya membangun kemitraan publik-swasta yang efektif untuk mengamankan infrastruktur, di mana kurangnya perjanjian formal dan mekanisme berbagi informasi menghambat kerja sama (Saputra et al., 2019).
3. Kesenjangan Regulasi dan Kapasitas: Perbandingan dengan negara seperti Jerman menunjukkan bahwa Indonesia masih tertinggal dalam membangun kerangka hukum dan kapasitas kelembagaan yang komprehensif untuk menghadapi ancaman canggih seperti spionase siber (Susila & Salim, 2024). Kesenjangan ini memperlambat internalisasi ancaman siber sebagai prioritas keamanan nasional yang mendesak.

Politik kebijakan keamanan siber Indonesia terjebak dalam paradoks: memiliki kesadaran strategis di tingkat makro tetapi menghadapi kendala implementasi yang berat di tingkat mikro. Hambatan struktural seperti fragmentasi kelembagaan, keterbatasan sumber daya, dan model kemitraan yang belum matang menghalangi terwujudnya postur keamanan siber yang tangguh dan proaktif.

Konflik dan Konvergensi Kepentingan

Politik kebijakan keamanan siber Indonesia merupakan arena tarik-menarik dinamis antara tiga poros kepentingan utama: keamanan nasional, ekonomi digital, dan hak-hak sipil. Analisis terhadap perumusan regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan wacana Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) mengungkap bahwa keseimbangan di antara kepentingan-kepentingan ini belum stabil. Terdapat ketegangan yang melekat, dan kepentingan keamanan nasional—khususnya yang diusung oleh aktor negara dengan perspektif keamanan tradisional—cenderung dominan dalam membentuk arah kebijakan, meskipun dengan resistensi dari koalisi kepentingan lain (Priyandita & Lebang, 2025; Susila & Salim, 2024).

Tarik-Menarik Kepentingan dalam Regulasi Siber

1. Keamanan Nasional vs. Ekonomi Digital: Perdebatan utama terletak pada tingkat kontrol negara terhadap aliran data dan infrastruktur digital. Konsep kedaulatan data (*data sovereignty*) dan lokalisasi data, yang kerap muncul dalam wacana kebijakan, didorong oleh kepentingan keamanan nasional untuk mengurangi ketergantungan pada penyedia asing dan memudahkan akses penegak hukum. Namun, ini berpotensi berbenturan dengan kepentingan ekonomi digital yang memerlukan arus data lintas batas yang lancar untuk mendukung inovasi, investasi asing, dan partisipasi dalam rantai pasok global. Regulasi yang terlalu restriktif dapat dianggap sebagai hambatan berusaha dan meningkatkan biaya operasi bagi perusahaan teknologi, baik lokal maupun multinasional (Saputra et al., 2019). Pemerintah, dalam hal ini, berusaha menjalankan peran ganda sebagai pelindung keamanan dan fasilitator ekonomi, yang menciptakan ambivalensi kebijakan.
2. Keamanan Nasional vs. Hak Sipil (Privasi): Ketegangan paling jelas terlihat dalam perumusan kebijakan yang melibatkan pengawasan (*surveillance*) dan akses data. UU PDP adalah sebuah kemajuan besar dalam mengakui hak privasi sebagai hak fundamental. Namun, implementasinya akan diuji oleh pasal-pasal yang mengizinkan pemrosesan data untuk "kepentingan penegakan hukum" dan "keamanan nasional" tanpa pengawasan peradilan yang ketat dan definitif yang jelas (Anwary, 2022). Sementara itu, wacana RUU KKS dikhawatirkan oleh kelompok masyarakat sipil dapat memperluas kewenangan agensi keamanan dan intelijen untuk melakukan pemantauan jaringan dan akses data secara real-time dengan dalih ancaman strategis. Di sini, logika sekuritisasi—yang membingkai ancaman siber sebagai isu eksistensial—digunakan untuk membenarkan pembatasan hak privasi dan potensi pengawasan masif (Bhakti et al., 2024).
3. Ekonomi Digital vs. Hak Sipil (Kebebasan Berekspresi): Kepentingan ekonomi digital yang mendorong platform untuk memoderasi konten secara agresif guna menciptakan "lingkungan digital yang aman" bagi pengiklan dan konsumen, dapat sejalan dengan kepentingan keamanan

nasional untuk menekan konten radikal atau hoaks. Namun, hal ini berisiko mereduksi ruang kebebasan berekspresi. Ketidakjelasan definisi konten "terlarang" atau "berbahaya" dalam undang-undang seperti UU ITE menciptakan ketidakpastian hukum dan berpotensi disalahgunakan untuk membungkus kritik, sehingga merugikan baik hak sipil maupun iklim bisnis dalam jangka panjang.

Aktor Dominan: Militer dan Paradigma Keamanan Negara yang Menguat

Analisis terhadap proses politik menunjukkan bahwa dalam tarik-menarik kepentingan ini, koalisi yang terdiri dari aktor-aktor dengan paradigma keamanan negara tradisional (terutama militer/TNI dan intelijen) memiliki pengaruh yang signifikan dan semakin menguat dalam membingkai arah kebijakan keamanan siber strategis (Priyandita & Lebang, 2025).

a. Pengaruh Militer dan Keamanan: TNI dan komunitas intelijen memiliki kapabilitas institusional yang mapan, akses langsung ke pembuat keputusan tertinggi, serta narasi yang kuat tentang "ancaman kedaulatan" yang mudah diterima dalam konteks politik. Wacana tentang "perang siber" dan kebutuhan untuk membangun kekuatan siber ofensif sebagai bagian dari deterensi banyak didorong oleh aktor-aktor ini (Bhakti et al., 2024). Pengaruh ini terlihat dalam pembentukan Pusat Siber TNI dan dorongan untuk memberikan mandat yang kuat kepada agensi negara dalam RUU KKS, yang sering kali mengesampingkan pertimbangan hak sipil dan checks and balances.
b. Peran Kepolisian: Polri dominan dalam domain kebijakan *cybercrime*, dengan kepentingan untuk memperluas kewenangan investigasi digital. Kepentingan mereka sering kali sejalan dengan militer dalam hal perluasan akses data, meski dengan fokus pada penegakan hukum pidana daripada perang siber (Anwary, 2022).
c. Aktor dengan Pengaruh Terbatas:
    1) Ekonom dan Pelaku Industri: Meski memiliki kepentingan besar, pengaruh mereka sering kali reaktif—berupaya melobi untuk melonggarkan aturan yang dianggap menghambat bisnis—daripada proaktif membingkai agenda kebijakan secara keseluruhan. Suara mereka lebih kuat dalam kebijakan sektoral (seperti perdagangan) dibandingkan dalam kebijakan keamanan siber inti (Saputra et al., 2019).
    2) Aktivis dan Masyarakat Sipil: Kelompok ini berperan penting sebagai *watchdog* dan berhasil memasukkan prinsip-prinsip hak asasi manusia ke dalam UU PDP. Namun, kapasitas advokasi mereka sering kali terbatas pada tahap sosialisasi RUU dan judicial review, dengan pengaruh yang minim dalam tahap perumusan awal kebijakan keamanan yang tertutup dan didominasi oleh aktor keamanan (Susila & Salim, 2024).

Konvergensi yang Rapuh

Meski tampak bertentangan, terkadang terjadi konvergensi kepentingan. Misalnya, perlindungan infrastruktur kritis adalah titik temu di mana kepentingan keamanan nasional (menjaga stabilitas negara), ekonomi digital (menjamin kelangsungan layanan bisnis), dan hak sipil (melindungi nyawa dan data warga) dapat bertemu. Namun, konvergensi ini rapuh karena setiap pihak memiliki prioritas dan metode yang berbeda. Negara mungkin menekankan kontrol dan standardisasi paksa, pelaku industri mengutamakan fleksibilitas dan efisiensi biaya, sementara masyarakat sipil menuntut transparansi dan akuntabilitas.

Politik keamanan siber Indonesia dicirikan oleh dominansi paradigma keamanan negara yang dibawa oleh aktor militer dan keamanan. Kepentingan ekonomi dan hak sipil, meski ada dan diperjuangkan, sering kali ditempatkan sebagai pertimbangan sekunder atau menjadi "dampak ikutan" dari kebijakan yang dirancang untuk memenuhi logika keamanan nasional tradisional. Ketidakseimbangan ini berpotensi melahirkan regulasi yang represif, menghambat inovasi, dan pada akhirnya melemahkan ketahanan siber nasional yang justru memerlukan partisipasi dan kepercayaan dari seluruh pemangku kepentingan.

Pengaruh Konteks Strategis

Pilihan Indonesia untuk mengadopsi model tata kelola siber yang multi-lembaga, kooperatif, dan berbasis aturan tidak dapat dipisahkan dari konteks strategis domestik dan internasionalnya. Model ini merupakan cerminan sekaligus hasil negosiasi dari identitas negara sebagai demokrasi terbesar ketiga di dunia dan middle power yang aktif di kancah diplomasi global (Priyandita & Lebang, 2025). Konteks ini membentuk sekaligus membatasi pilihan kebijakan keamanan siber Indonesia.

Konteks Domestik: Demokrasi, Desentralisasi, dan Fragmentasi

Struktur politik dan sosial Indonesia dalam negeri secara langsung membentuk kerangka tata kelola sibernya yang kompleks.

1. Sistem Politik Demokrasi Multipartai: Demokrasi Indonesia, dengan parlemen yang aktif dan kebebasan pers yang dinamis, menciptakan ruang publik yang vokal untuk mengkritik kebijakan. Hal ini mencegah pendekatan keamanan siber yang terlalu tertutup dan otoriter, seperti yang terjadi di Iran. Setiap upaya untuk memberlakukan regulasi yang dipersepsikan membatasi hak, seperti RUU KKS, akan menghadapi scrutini publik dan perdebatan parlemen yang intens (Anwary, 2022). Namun, demokrasi juga berarti kebijakan adalah hasil kompromi politik. Model multi-lembaga yang ada—dengan pembagian wewenang antara BSSN, Polri, dan TNI—sebagian merupakan kompromi untuk mengakomodasi kepentingan berbagai faksi dalam birokrasi dan politik, meski sering mengorbankan efisiensi dan kejelasan komando (Priyandita & Lebang, 2025).
2. Kebijakan Desentralisasi: Otonomi daerah telah mentransfer banyak kewenangan pelayanan publik dan pengelolaan data kependudukan ke tingkat kabupaten/kota. Namun, hal ini justru memperparah kesenjangan kapasitas keamanan siber secara nasional. Pemerintah daerah umumnya kekurangan anggaran, SDM, dan kesadaran untuk menerapkan standar keamanan siber nasional. Kerentanan sistem informasi daerah menjadi titik lemah (*weak link*) dalam pertahanan siber nasional, sekaligus menjelaskan mengapa pendekatan koordinatif BSSN (seperti melalui CSIRT daerah) menjadi satu-satunya pilihan yang realistis, meski lambat, daripada model komando terpusat yang tidak feasible secara politis dan administratif.
3. Keragaman Sosial Budaya: Masyarakat Indonesia yang majemuk dengan tensi sosial yang periodik menciptakan kerentanan unik terhadap perang informasi dan disinformasi. Ancaman seperti ujaran kebencian bermuatan SARA dan hoaks yang menggerus kohesi sosial menjadi prioritas dalam perspektif keamanan dalam negeri. Ini menjelaskan mengapa Polri memiliki peran besar dan mengapa narasi kebijakan sering kali menekankan "ketertiban" dan "kerukunan" di ruang digital, yang terkadang berpotensi berbenturan dengan kebebasan berekspresi.

Konteks Internasional: Middle Power dan Diplomasi Normatif

Posisi dan identitas Indonesia di panggung dunia secara fundamental membentuk postur kebijakan sibernya menjadi lebih kooperatif dan hati-hati.

1. Kepemimpinan dan Norma di ASEAN: Indonesia secara konsisten memposisikan diri sebagai penjaga stabilitas dan penengah (*honest broker*) di ASEAN. Melalui forum seperti ASEAN Ministerial Conference on Cybersecurity (AMCC) dan ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), Indonesia aktif mendorong kerja sama kapasitas, berbagi informasi ancaman, dan pembentukan norma perilaku negara di ruang siber di tingkat regional (Susila & Salim, 2024). Keterlibatan ini bukan hanya soal keamanan teknis, tetapi juga proyeksi soft power untuk memperkuat kepemimpinan Indonesia. Postur ini membuat Indonesia cenderung menolak pendekatan konfrontatif atau militeristik murni dalam siber, karena bertentangan dengan prinsip-prinsip konsensus dan non-intervensi yang menjadi fondasi ASEAN.
2. Komitmen pada Tata Kelola Siber Global Berbasis Aturan: Sebagai anggota PBB yang aktif, Indonesia secara resmi mendukung proses United Nations Group of Governmental Experts (UNGGE) dan Open-Ended Working Group (OEWG) yang mengadvokasi penerapan hukum internasional dan norma-norma kesopanan (*norms of responsible state behavior*) di ruang siber.

Komitmen pada "rules-based international order" ini berfungsi sebagai pembatas strategis terhadap perkembangan doktrin siber yang terlalu ofensif. Indonesia, sebagai negara yang secara tradisional menentang intervensi asing, memiliki kepentingan untuk membatasi ruang gerak negara-negara besar dalam melakukan serangan siber. Oleh karena itu, pendekatan kebijakannya lebih condong pada deterensi melalui ketahanan (*resilience*) dan diplomasi hukum internasional, dibandingkan pembangunan kekuatan balasan (*retaliatory*) secara terbuka (Bhakti et al., 2024).

3. Ketegangan antara Kedaulatan dan Interkoneksi: Konteks internasional juga memperkuat ketegangan domestik antara kedaulatan dan keterbukaan. Di satu sisi, Indonesia ingin melindungi data warganya dan infrastruktur kritisnya dari pengaruh asing (kedaulatan siber). Di sisi lain, sebagai ekonomi digital yang sedang tumbuh dan anggota G20, Indonesia bergantung pada arus data dan investasi teknologi global. Tarik-menarik ini menjelaskan ambivalensi dalam kebijakan: dukungan pada norma global di satu forum, sementara merumuskan aturan lokalisasi data yang potensial protektif di dalam negeri.

Konteks strategis domestik dan internasional Indonesia berfungsi sebagai dua sisi mata uang yang sama. Konteks domestik (demokrasi, desentralisasi) *memaksa* negara untuk mengadopsi model tata kelola yang inklusif dan terfragmentasi, sementara konteks internasional (middle power diplomacy) *mendorong* negara untuk memilih pendekatan kooperatif dan berbasis norma. Kombinasi ini menghasilkan postur keamanan siber Indonesia yang unik: lebih defensif dan diplomatik daripada ofensif dan unilateral, namun diwarnai oleh kompleksitas dan inefisiensi internal yang menjadi harga yang harus dibayar bagi demokrasi yang besar dan desentralistik.

Restrukturisasi Aktor dan Kelembagaan Pasca-Krisis

Serangan Stuxnet pada 2010 tidak hanya berdampak pada fasilitas nuklir Natanz, tetapi juga berfungsi sebagai *focusing event* yang mentransformasi secara radikal politik dan arsitektur kelembagaan keamanan siber Iran. Berbeda dengan model multi-lembaga Indonesia, respons Iran terhadap krisis ini dicirikan oleh konsolidasi kekuasaan yang cepat dan absolut ke dalam tangan tubuh militer dan intelijen, khususnya Korps Garda Revolusi Islam (IRGC), yang secara efektif memonopoli otoritas strategis di ruang siber (Shakarian, 2013; Kumar,. 2025).

Konsolidasi Kekuasaan: Monopoli Militer-Intelijen atas Ranah Siber

Stuxnet memaparkan kerentanan eksistensial Iran terhadap serangan siber canggih dari musuh negara, yang langsung dimanfaatkan oleh aktor-aktor dengan paradigma keamanan paling keras. Dominasi Korps Garda Revolusi Islam (IRGC): Sebelum Stuxnet, tata kelola siber Iran relatif terfragmentasi. Pasca-serangan, IRGC—sebagai tulang punggung ideologis dan keamanan rezim—dengan cepat memperluas mandatnya. IRGC tidak hanya bertanggung jawab atas keamanan fisik fasilitas strategis, tetapi juga mengambil alih kepemimpinan dalam membangun kapabilitas siber defensif dan ofensif nasional (Shakarian, 2013). Unit khusus seperti Komando Siber IRGC dibentuk, yang bertugas melindungi infrastruktur kritis dan melaksanakan operasi siber. Dominasi ini mencerminkan persepsi ancaman yang menyeluruh: ruang siber dipandang sebagai medan tempur baru (*new warfare domain*) yang terlalu penting untuk diserahkan kepada lembaga sipil.

Peran Badan Intelijen: Badan intelijen, termasuk Ministry of Intelligence and Security (MOIS), juga memperkuat perannya dalam pengawasan siber domestik dan operasi luar negeri. Sinergi antara IRGC dan badan intelijen menciptakan sebuah kompleks militer-intelijen siber yang kuat, dengan garis komando yang terpusat dan langsung bertanggung jawab kepada Pemimpin Tertinggi (*Supreme Leader*). Struktur ini memungkinkan mobilisasi sumber daya dan eksekusi kebijakan dengan kecepatan dan kerahasiaan yang tidak mungkin dicapai dalam sistem demokratis yang terdesentralisasi.

Marginalisasi Aktor Sipil: Teknokrat dan Akademisi dalam Bayangan Militer

Transformasi pasca-Stuxnet ditandai dengan semakin tersingkir atau tersubordinasi-nya aktor-aktor sipil dari pusat pengambilan keputusan strategis siber. Subordinasi Kementerian Teknis: Kementerian-kementerian teknis sipil, seperti Kementerian Teknologi Informasi dan Komunikasi

(ICT), yang sebelumnya memegang peran regulasi di ruang digital, secara efektif kehilangan pengaruhnya dalam masalah kebijakan siber strategis. Peran mereka direduksi menjadi pelaksana teknis dan regulator isu-isu non-keamanan, seperti pengembangan infrastruktur broadband. Keputusan-keputusan penting mengenai doktrin, anggaran, dan operasi siber diambil di dalam lingkaran tertutup IRGC dan Dewan Keamanan Tertinggi Nasional (SCNS) (Kumar, Tripathi, & Das, 2025).

Instrumentalisasi Komunitas Akademik: Berbeda dengan Indonesia di mana akademisi seringkali terpinggirkan secara pasif, di Iran komunitas teknis dan akademik sipil justru diinstrumentalisasi secara aktif oleh negara. Bakat-bakat siber direkrut secara agresif melalui program nasional dan diarahkan untuk mendukung agenda keamanan negara. Universitas-universitas dikerahkan untuk meningkatkan program pendidikan siber, tetapi kurikulum dan penelitiannya harus selaras dengan prioritas keamanan nasional yang ditetapkan oleh militer. Kebebasan akademik dan kritik independen terhadap kebijakan siber negara praktis tidak ada. Model ini menciptakan *brain gain* bagi negara tetapi dengan mengorbankan ekosistem inovasi sipil yang otonom dan kritis.

Pembentukan Unit-Unit Siber Khusus dan Doktrin Baru

Restrukturisasi kelembagaan berjalan seiring dengan pembentukan doktrin operasional baru.

1. Spesialisasi dan Segmentasi: IRGC membentuk unit-unit siber yang tersegmentasi berdasarkan fungsi, misalnya unit yang fokus pada perang informasi dan propaganda, unit yang menargetkan infrastruktur kritis negara musuh, dan unit untuk pertahanan infrastruktur domestik (Shakarian, 2013).
2. Doktrin "Pertahanan Aktif" (*Active Defense*): Stuxnet membuktikan bahwa pertahanan pasif tidak cukup. Iran kemudian mengadopsi doktrin yang mencampurkan pertahanan dengan kapabilitas ofensif sebagai bentuk deterensi dan pembalasan (*retaliation*). Pembentukan kekuatan siber ofensif di bawah komando militer menjadi inti dari doktrin ini, yang bertujuan untuk meningkatkan biaya bagi musuh yang ingin menyerang Iran (Kumar, Tripathi, & Das, 2025).

Stuxnet berfungsi sebagai katalis yang mengakhiri ambiguitas kelembagaan di Iran. Ancaman eksistensial yang ditimbulkannya digunakan untuk melegitimasi konsolidasi kekuasaan yang belum pernah terjadi sebelumnya oleh kompleks militer-intelijen, meminggirkan suara sipil, dan menciptakan struktur komando siber yang terpusat, rahasia, dan siap tempur. Model "keamanan nasional di atas segalanya" ini berdiri dalam kontras yang sangat tajam dengan model Indonesia yang demokratis namun terfragmentasi.

Proses Kebijakan: Sekuritisasi dan Mobilisasi Cepat

Stuxnet bukan hanya serangan teknis terhadap fasilitas nuklir Natanz, tetapi juga sebuah "peluang politik" yang dimanfaatkan secara maksimal oleh rezim Iran. Melalui proses sekuritisasi—pembingkaian suatu isu sebagai ancaman eksistensial yang memerlukan tindakan luar biasa dan darurat—elit keamanan Iran mentransformasi kejutan Stuxnet menjadi landasan untuk mobilisasi sumber daya dan restrukturisasi kebijakan secara masif, cepat, dan tertutup. Proses ini terjadi dengan mekanisme yang hampir berlawanan dengan model konsultatif dan birokratis di Indonesia (Kumar, Tripathi, & Das, 2025; Loukas, 2015).

Stuxnet sebagai Catalyst: Narasi "Perang Siber" dan Ancaman Eksistensial

Narasi resmi yang dibangun pasca-Stuxnet sangatlah kuat dan bertujuan tunggal: melegitimasi setiap langkah yang diambil.

1. Pembingkaian sebagai "Serangan Perang": Pemerintah dan media negara dengan segera membingkai Stuxnet bukan sebagai kejahatan siber (*cybercrime*) atau bahkan sekadar spionase, melainkan sebagai "serangan perang" (*act of war*) yang dilakukan oleh musuh-musuh negara (terutama Amerika Serikat dan Israel) (Loukas, 2015). Narasi ini menekankan sifatnya yang *state-sponsored*, canggih, dan ditujukan untuk menghancurkan aset kedaulatan nasional (program nuklir). Dengan demikian, ancaman tersebut diposisikan setara dengan serangan militer

konvensional, yang secara otomatis memanggil otoritas dan legitimasi tertinggi dari institusi militer dan keamanan.

2. Konstruksi "Ancaman Eksistensial": Lebih jauh, Stuxnet digambarkan sebagai ancaman terhadap kelangsungan rezim dan keamanan nasional. Kemampuan malware untuk menyusup dan merusak tanpa terdeteksi menciptakan narasi tentang kerentanan total dan ketidakberdayaan. Narasi ini berfungsi sebagai *rallying cry* internal untuk menutupi perdebatan, menekan kritik, dan menyatukan berbagai faksi di bawah panji perlawanan terhadap musuh eksternal. Keterbukaan terhadap dunia luar—baik dalam bentuk kerja sama internasional, teknologi asing, atau arus informasi—dipandang sebagai risiko keamanan yang tidak dapat diterima (Kumar, Tripathi, & Das, 2025).

4. KESIMPULAN, KETERBATASAN DAN SARAN

Kesimpulan

Kesimpulan penelitian ini menunjukkan bahwa kesiapan keamanan siber Indonesia dalam menghadapi ancaman strategis seperti Stuxnet masih bersifat reaktif, terfragmentasi, dan belum sepenuhnya tangguh dibandingkan Iran yang mampu melakukan transformasi cepat melalui sistem komando terpusat. Indonesia menghadapi kendala koordinasi antar lembaga, keterbatasan sumber daya, serta kesenjangan implementasi kebijakan. Namun demikian, pendekatan Indonesia yang berbasis demokrasi, hukum, dan kerja sama internasional menjadi kekuatan jangka panjang dalam membangun ketahanan siber yang berkelanjutan. Sementara itu, Iran menunjukkan efektivitas tinggi dalam mobilisasi dan penguatan kapasitas siber, tetapi dengan konsekuensi berkurangnya kebebasan sipil dan meningkatnya militerisasi ruang siber. Oleh karena itu, Indonesia perlu mengambil pembelajaran fungsional dari Iran, terutama dalam aspek kejelasan komando dan pengembangan SDM, tanpa meninggalkan prinsip demokrasi dan hak asasi manusia.

Keterbatasan

Keterbatasan penelitian ini terletak pada penggunaan pendekatan kualitatif komparatif yang sangat bergantung pada data sekunder dan literatur akademik sehingga belum sepenuhnya menggambarkan dinamika operasional keamanan siber secara langsung di lapangan. Selain itu, penelitian ini hanya berfokus pada perbandingan Indonesia dan Iran pasca-Stuxnet sehingga belum mencakup variasi model keamanan siber negara lain yang mungkin memiliki karakteristik berbeda. Keterbatasan akses terhadap data strategis dan informasi keamanan yang bersifat rahasia juga menjadi kendala dalam memperoleh gambaran yang lebih komprehensif mengenai kapasitas nyata kedua negara.

Saran

Saran penelitian ini menekankan pentingnya penguatan tata kelola keamanan siber Indonesia melalui peningkatan kewenangan operasional BSSN, pembentukan mekanisme koordinasi terpadu antar lembaga, serta penguatan kemitraan pemerintah dan sektor swasta dalam perlindungan infrastruktur kritis. Pemerintah juga perlu mempercepat pengembangan SDM dan riset keamanan siber nasional melalui investasi pendidikan, inovasi teknologi, dan kolaborasi internasional. Selain itu, Indonesia perlu memperkuat strategi ketahanan siber berbasis deteksi dini, pemulihan cepat, dan diplomasi siber aktif di tingkat regional maupun global agar mampu menghadapi ancaman siber strategis secara lebih efektif tanpa mengorbankan prinsip demokrasi dan perlindungan hak asasi manusia.

DAFTAR PUSTAKA

Abdillah, A., Widianingsih, I., Buchari, R., & Nurasa, H. (2024). Big data security & individual (psychological) resilience: A review of social media risks and lessons learned from Indonesia. *Array, 21*, 100336.

Anwary, I. (2022). The role of public administration in combating cybercrime: An analysis of the legal framework in Indonesia. *International Journal of Cyber Criminology, 16*(2), 216–227.

Bhakti, A., Sudirman, A., Widya, S. S. 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.

Hossain, S., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance, 5*, 100091.

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis, 59*(1), 111–128.

Kumar, S., Tripathi, K., & Das, S. (2025). Cybersecurity of energy systems. *Methods in Chemical Process Safety, 9*.

Loukas, G. (2015). A history of cyber-physical security incidents. In *Cyber-Physical Attacks* (pp. 35–62). Elsevier.

Ponnusamy, V., Jhanjhi, N. Z., & Humayun, M. (2019). Fostering public-private partnership: Between governments and technologists in developing national cybersecurity framework. In *Employing recent technologies for improved digital governance* (pp. 237–255).

Priyandita, G., & Lebang, C. G. (2025). Constrained cyber power: Authoritarian legacies on Indonesia's cyber capabilities development. *Journal of Information Technology & Politics*.

Raja, M., Masood, Z., Hussain, I., Zameer, A., & Raja, M. (2025). Design of deep learning networks for nonlinear delay differential system for Stuxnet virus spread in an air gapped critical environment. *Applied Soft Computing, 175*, 113091.

Rid, T. (2022). *Cyber war will not take place*. Oxford University Press.

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's cyber security through public-private partnership (PPP). *Central European Journal of International and Security Studies, 13*(4), 104–120.

Sen, Ö., van der Velde, D., Wehrmeister, K., Hacker, I., Henze, M., & Andres, M. (2022). On using contextual correlation to detect multi-stage cyber attacks in smart grids. *Sustainable Energy, Grids and Networks, 32*, 100821.

Shakarian, P. (2013). Attacking Iranian nuclear facilities: Stuxnet. In *Introduction to Cyber-Warfare* (pp. 261–280). Syngress.

Susila, M. E., & Salim, A. A. (2024). Cyber espionage policy and regulation: A comparative analysis of Indonesia and Germany. *Padjadjaran Jurnal Ilmu Hukum, 11*(1), 122–144.

Ulum, M. (2026). *Buku Politik Keamanan Siber*. UMJ Press.

Wahyudi, R., Marjaka, W., Silangen, C., Supriatna, J., Fajar, M., Winarni, N., & Dharmawan, I. (2025). Advancing Mutual Recognition Agreements (MRAs) between Indonesia's SRN and international standards to expand forestry carbon credits in VCMs. *Trees, Forests and People, 22*, 101017.

Willis, R., & Sidabutar, J. (2024). How can Gov-CSIRT Indonesia maintain national cybersecurity in the future? In *Proceedings of the 16th International Conference on Information Technology and Electrical Engineering (ICITEE 2024)* (pp. 440–445).

Zhen, Z., & Gao, J. (2023). Chinese Cyber Threat Intelligence Named Entity Recognition via RoBERTa-wwm-RDCNN-CRF. *Computers, Materials and Continua, 77*(1), 1203–1222.