ANALISIS STRATEGI KEAMANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN RANSOMWARE: STUDI KASUS SEKTOR LAYANAN PUBLIK DAN PERBANKAN, 2020—2024

(Skripsi)

Oleh

ELNAYA PRICILIA

NPM 2216071102

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2026

ABSTRAK

ANALISIS STRATEGI KEAMANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN RANSOMWARE: STUDI KASUS SEKTOR LAYANAN PUBLIK DAN PERBANKAN, 2020—2024

Oleh

ELNAYA PRICILIA

Keamanan siber merupakan salah satu sektor penting bagi Indonesia. Namun, seiring perubahan lanskap ancaman global, Indonesia kini mengembangkan segmen mitigasi yang lebih spesifik, seperti *financial-sector cybersecurity* dan *public-service cloud security* guna menegakkan kedaulatan digital nasional secara menyeluruh.

Penelitian ini menganalisis strategi keamanan siber Indonesia terhadap eskalasi ancaman ransomware transnasional periode 2020–2024 dengan studi kasus serangan LockBit 3.0 pada Bank Syariah Indonesia (2023) dan Brain Cipher pada Pusat Data Nasional Sementara 2 (2024). Menggunakan pendekatan kualitatif deskriptif, penelitian ini mengevaluasi upaya keamanan Indonesia melalui lensa Teori Strategi Keamanan Siber Nasional dan Konsep Tata Kelola Keamanan Siber Nasional. Data sekunder bersumber dari laporan resmi BSSN dan dokumen kebijakan dianalisis menggunakan teknik kondensasi, penyajian, dan triangulasi sumber.

Hasil penelitian menunjukkan bahwa implementasi 5 Pilar ITU di Indonesia masih menemui kendala pada aspek teknis dan organisasi, terutama terkait *compliance gap* instansi pemerintah serta fragmentasi otoritas antarlembaga yang menghambat respons cepat terhadap serangan siber. Akibatnya, aktor eksternal masih dapat mengeksploitasi celah keamanan pada sektor publik dan perbankan karena belum terwujudnya integrasi yang utuh di kelima pilar tersebut. Penelitian menyimpulkan bahwa penguatan kedaulatan digital memerlukan sinkronisasi komando kelembagaan yang tersentralisasi, ketegasan sanksi hukum atas kelalaian risiko, serta kedisiplinan operasional yang ketat guna mewujudkan ekosistem data publik yang resiliens.

Kata kunci: Keamanan Siber, *Ransomware*, 5 Pilar ITU, BSI, PDNS 2.

ABSTRACT

ANALYSIS OF INDONESIA'S CYBER SECURITY STRATEGY AGAINST RANSOMWARE ATTACKS: A CASE STUDY OF THE PUBLIC SERVICE AND BANKING SECTORS, 2020—2024

By

ELNAYA PRICILIA

Cybersecurity is one of the crucial sectors for Indonesia. However, along with the shifting global threat landscape, Indonesia is now developing more specific mitigation segments, such as financial-sector cybersecurity and public-service cloud security, in order to enforce national digital sovereignty comprehensively.

This research analyzes Indonesia's cybersecurity strategy against the escalation of transnational ransomware threats during the 2020–2024 period, focusing on the case studies of the LockBit 3.0 attack on Bank Syariah Indonesia (2023) and the Brain Cipher attack on the Temporary National Data Center 2 (2024). Utilizing a descriptive qualitative approach, this study evaluates Indonesia's cybersecurity efforts through the lens of National Cybersecurity Strategy Theory and National Cybersecurity Governance Concepts. Secondary data derived from official BSSN reports and policy documents were analyzed using data condensation, data display, and source triangulation techniques.

The results indicate that the implementation of the 5 ITU Pillars in Indonesia still encounters obstacles in technical and organizational aspects, particularly regarding the compliance gap within government agencies and the fragmentation of authority among institutions, which hinders rapid responses to cyberattacks. Consequently, external actors are still able to exploit security vulnerabilities in the public and banking sectors due to the absence of full integration across these five pillars. The study concludes that strengthening digital sovereignty requires centralized institutional command synchronization, strict legal sanctions for risk negligence, and rigorous operational discipline to realize a resilient public data ecosystem.

Keywords: *Cybersecurity*, *Ransomware*, ITU 5 Pillars, BSI, PDNS 2.

ANALISIS STRATEGI KEAMANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN RANSOMWARE: STUDI KASUS SEKTOR LAYANAN PUBLIK DAN PERBANKAN, 2020—2024

Oleh

ELNAYA PRICILIA

SKRIPSI

Sebagai Salah Satu Syarat untuk Mencapai Gelar

SARJANA HUBUNGAN INTERNASIONAL

Pada

Jurusan Hubungan Internasional

Fakultas Ilmu Sosial dan Ilmu Politik

JURUSAN HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS LAMPUNG

2026

Judul Skripsi	:	**ANALISIS STRATEGI KEAMANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN RANSOMWARE: STUDI KASUS SEKTOR LAYANAN PUBLIK DAN PERBANKAN, 2020-2024**
Nama Mahasiswa	:	**Elnaya Pricilia**
Nomor Pokok Mahasiswa	:	**2216071102**
Jurusan	:	**Hubungan Internasional**
Fakultas	:	**Ilmu Sosial dan Ilmu Politik**

MENYETUJUI

1. Komisi Pembimbing

Iwan Sulistyo, S.Sos., M.A.
NIP. 19860428 201504 1 004

2. Ketua Jurusan Hubungan Internasional

Dr. Simon Sumajoyo H. S.A.N., M.PA.
NIP. 19810628 200501 1 003

MENGESAHKAN

1. **Tim Penguji**

   Ketua : **Iwan Sulistyo, S.Sos., M.A.** .....

   Penguji Utama : **Gita Karisma, S.IP., M.Si.** .....

2. **Dekan Fakultas Ilmu Sosial dan Ilmu Politik**

Prof. Dr. Anna Agustina Zainal, S.Sos., M.Si.
NIP. 19760821 200003 2 001

Tanggal Lulus Ujian Skripsi: **8 Juni 2026**

PERNYATAAN

Dengan ini saya menyatakan bahwa

1. Karya tulis saya, skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana), baik di Universitas Lampung maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan komisi pembimbing dan penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan sebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah berlaku di Universitas Lampung.

Bandarlampung, 2 Juni 2026
Yang membuat pernyataan,

Elnaya Pricilia
2216071102

RIWAYAT HIDUP

Penulis memiliki nama lengkap Elnaya Pricilia, dilahirkan di Tulang Bawang pada 11 Oktober 2003 dari pasangan Bapak Dwi Supriantoro dan Ibu Siluh Putu Sudewi. Penulis merupakan anak terakhir dari dua bersaudara. Penulis mengawali perjalanan akademisnya di TK 04 Yapindo dan SD 02 Yapindo, kemudian penulis melanjutkan studinya ke jenjang SMP Yapindo dan SMAS Sugar Group B Mataram. Pada tahun 2022, penulis melanjutkan pendidikan tinggi di program studi S-1 Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Lampung. Kesempatan studi tersebut penulis raih melalui jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN). Selama menempuh studi di Universitas Lampung penulis aktif melibatkan diri dalam berbagai kegiatan baik di tingkat jurusan maupun di tingkat universitas.

Selama menempuh studi di Universitas Lampung, penulis aktif mengikuti berbagai kegiatan, baik di tingkat jurusan maupun universitas. Di lingkup universitas, penulis bergabung dengan Unit Kegiatan Mahasiswa (UKM) yang berfokus pada bidang penyiaran, yakni Radio Kampus Universitas Lampung (RAKANILA) dari tahun 2022–2025. Penulis tidak hanya berkontribusi sebagai anggota, tetapi juga dipercaya untuk mengemban amanah sebagai pengurus dalam struktur organisasi, yakni menjabat sebagai Kepala Divisi *Creative* pada periode 2023–2024 dan Kepala Divisi *Off Air* pada periode 2024–2025. Selain aktif di tingkat universitas, penulis juga aktif mengikuti kegiatan di jurusan, seperti menjadi *Liaison Officer* (LO) pada Funcamp HI Unila 2023 dan Pertemuan Nasional Mahasiswa Hubungan Internasional Se-Indonesia (PNMHII) ke-36 pada tahun 2024. Kemudian pada tahun 2025, penulis mengikuti KKN MBKM selama 30 hari di desa Kerinjing, Kabupaten Lampung Selatan.

MOTTO

"*Sesungguhnya Allah mencintai amalan seseorang di antara kalian yang apabila ia melakukan suatu pekerjaan, maka ia menyelesaikannya dengan baik (itqan)*."

(HR. Abu Dawud dan Tirmidzi)

"It's okay to fall, it's okay to make mistakes. It's because those moments are the ones that make us who we are."

(Min Yoongi)

"Tugas kita bukanlah untuk berhasil. Tugas kita adalah untuk mencoba, karena didalam mencoba itulah kita menemukan dan belajar membangun kesempatan untuk berhasil."

(Buya Hamka)

PERSEMBAHAN

Untuk Ayah, Ibu, Kakak, keluarga yang penulis

sayangi, dan seluruh pembaca

SANWACANA

Segala puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas seluruh limpahan berkah dan petunjuk-Nya, sehingga penulis dapat merampungkan draf Tugas Akhir yang berjudul "Analisis Strategi Keamanan Siber Indonesia dalam Menghadapi Ancaman Ransomware: Studi Kasus Sektor Layanan Publik dan Perbankan, 2020—2024" dengan baik. Penulisan draf ini diselesaikan guna memenuhi salah satu syarat akademis dalam memperoleh gelar Sarjana Hubungan Internasional pada Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Lampung. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya atas segala bimbingan, doa, serta motivasi selama proses penyusunan draf ini, kepada:

1. Kedua orang tua penulis, Bapak Dwi Supriantoro dan Ibu Siluh Putu Sudewi. Ungkapan terima kasih yang tak terhingga penulis persembahkan atas seluruh pengorbanan, kesabaran, dan kepercayaan yang telah diberikan selama ini. Penulis bersyukur memiliki Bapak yang luar biasa, yang senantiasa hadir memberikan kekuatan baik dalam suka maupun duka di setiap tahapan proses yang penulis lalui. Di atas segalanya, rasa hormat dan tanda bakti paling mendalam penulis tujukan kepada Ibu, yang dengan ketangguhannya telah bekerja keras membanting tulang sendirian tanpa kenal lelah demi masa depan penulis. Tanpa doa dan cucuran keringat Ibu, penulis tidak akan pernah sampai di titik ini.
2. Kakak penulis, Nadhira Dewiantari, terima kasih atas segala bentuk kasih sayang, doa, dan kebaikan yang telah diberikan selama ini. Penulis sangat bersyukur atas ketulusan Kakak yang telah ikut membantu memfasilitasi kebutuhan kuliah penulis, selalu sabar menjadi tempat berbagi keluh kesah, dan senantiasa menjadi garda terdepan yang siap membela setiap kali penulis

menghadapi masalah. Setiap perhatian dan kepedulian yang Kakak berikan merupakan hal yang sangat berarti dalam keberhasilan penulis menyelesaikan studi ini.

3. Ibu Prof. Dr. Anna Gustina Zainal., M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.
4. Bapak Dr. Simon Sumanjoyo Hutagalung, S.A.N., M.P.A., selaku Ketua Jurusan Hubungan Internasional FISIP Universitas Lampung.
5. Mba Astiwi Inayah, S.IP., M.A., selaku Dosen Pembimbing Akademik, atas kesabaran dan kebaikan beliau dalam memberikan bimbingan serta motivasi kepada penulis selama menempuh studi di jurusan Hubungan Internasional.
6. Mas Iwan Sulistyo, S.Sos., M.A., selaku Dosen Pembimbing Utama, yang senantiasa sabar meluangkan waktu dan memberikan banyak masukan berharga. Terima kasih atas bimbingan, arahan, serta pengalaman baik secara intelektual maupun praktikal yang telah diberikan kepada penulis selama proses penyelesaian Tugas Akhir ini.
7. Mba Gita Karisma, S.IP.,M.Si. selaku Dosen Penguji. Penulis mengucapkan terima kasih yang sebesar-besarnya atas arahan, sudut pandang baru, dan motivasi yang beliau berikan. Setiap masukan yang disampaikan sangat berarti dalam memperbaiki kualitas Tugas Akhir ini agar menjadi lebih baik.
8. Seluruh dosen dan staf Jurusan Hubungan Internasional Universitas Lampung, terima kasih atas dedikasi, bimbingan, dan ilmu pengetahuan yang telah dibagikan selama penulis menempuh masa studi. Terima kasih juga kepada pihak staf jurusan atas bantuan administratif dan pelayanan baik yang diberikan dari awal perkuliahan hingga proses penyusunan Tugas Akhir ini selesai.
9. Yuanka Siwi Pramudya Hapsari dan Klara Meiva Nirmala, sahabat seperjuangan sejak kecil yang selalu ada dalam setiap fase pertumbuhan penulis dari Sekolah Dasar hingga sekarang. Terima kasih sudah selalu menyediakan waktu dan telinga di titik-titik terlelah penulis, menjadi tempat bersandar yang paling nyaman saat tekanan kuliah dan dinamika hidup terasa begitu berat.

10. Nanda Sahnaz, teman sejak masa SMA yang sangat berharga. Terima kasih karena selalu meluangkan waktu, setia menjadi tempat bertukar cerita di ruang obrolan, dan senantiasa hadir memberikan dukungan serta kehangatan di setiap fase perjalanan hidup penulis hingga saat ini.
11. Jihan Aqila Altaf Supollo, Tita Andina Sari, dan Talitha Adzani Lukman. Dari asingnya hari pertama menjadi mahasiswa baru hingga menjadi saksi perjuangan satu sama lain di akhir masa studi, Terima kasih telah menjadi bagian dari bab terpenting dalam hidup penulis selama di Universitas. Terima kasih atas solidaritas yang tiada batas, tawa yang mencairkan penat, serta kesediaan kalian untuk selalu saling menopang di tengah padatnya jadwal kuliah, tugas-tugas, dan revisi.
12. Ridho Pratama Putra, seorang lelaki yang hadir dalam hidup penulis sejak tahun 2024 hingga saat ini. Terima kasih karena selalu setia menemani dalam setiap suka maupun duka, serta atas kontribusi dan bantuan besarnya dalam penyusunan Tugas Akhir ini. Terima kasih atas segala kasih sayang, cinta, dan kesabaran yang telah diberikan selama ini.
13. Cindy Karelta, sosok teman yang selalu memberikan kenyamanan bagi penulis untuk berbagi cerita, tawa, hingga bertukar candaan di setiap waktu. Terima kasih telah menjadi ruang paling menyenangkan dan selalu berhasil membawa keceriaan.
14. Fathia Az-zahra, Afiyah Nur Kamilah, Rahmah Aulia, Cyntia Apriani Ambarita, dan Naila Fahsya Anindhiya, yang telah membersamai jejak langkah penulis dari nol sejak pertama kali menyandang status sebagai mahasiswa. Terima kasih banyak atas setiap momen kebersamaan, bantuan kecil yang saling meringankan, serta cerita-cerita spontan yang selalu berhasil mencairkan ketegangan dunia akademik.
15. Zahra Elfaya Nabil dan Keysya Romeins, dua teman sekaligus rekan seperjuangan yang telah membersamai penulis sejak masa-masa aktif di organisasi hingga akhir perjalanan akademik ini. Terima kasih yang tak

terhingga atas dedikasi, semangat, dan solidaritas yang telah kalian tunjukkan selama ini.

16. Rika Nurlaila Damayanti dan Bintang Surya Ramadhani, teman-teman seperjuangan terbaik dalam melewati setiap fase krusial mulai dari sempro, semhas, hingga kompre. Terima kasih telah menjadi rekan bertukar pikiran yang sangat membantu, saling menguatkan di kala cemas menghadapi ujian sidang, dan memastikan kita semua bisa melangkah bersama menuju kelulusan.
17. Desylfa ika shervia, teman baik dan rekan seperjuangan yang telah membersamai langkah penulis dari semester 2 hingga saat ini. Terima kasih atas ketulusan, kebersamaan, dan dukungan yang tiada henti dalam melewati setiap dinamika perkuliahan dari awal hingga titik kelulusan.
18. *Boyband* BTS, terima kasih telah menjadi salah satu alasan penulis untuk tetap bersemangat dan pantang menyerah dari tahun 2018 hingga detik kelulusan ini. Musik, dedikasi, dan energi positif yang mereka tunjukkan selalu berhasil menjadi penawar lelah di tengah padatnya aktivitas akademik dan penyusunan Tugas Akhir ini. Kehadiran mereka sebagai pemantik semangat memiliki arti tersendiri dalam ruang proses penulis.
19. Terakhir, sebuah apresiasi dan rasa terima kasih yang teramat dalam untuk diri saya sendiri. Terima kasih karena telah mampu berdiri dengan kuat, bertahan, dan tidak pernah menyerah dalam menyelesaikan Tugas Akhir ini hingga garis akhir. Meskipun harus melewati begitu banyak dinamika, peliknya perjuangan, dan air mata di sepanjang prosesnya, terima kasih karena selalu memilih untuk bangkit dan percaya pada kemampuan diri sendiri. Pencapaian ini adalah bukti nyata dari kerja keras dan ketangguhan yang selama ini telah diupayakan.

Bandar Lampung, 1 Juni 2026

Elnaya Pricilia

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

APT	: *Advanced Persistent Threat*
ASN	: Aparatur Sipil Negara
ATM	: *Automated Teller Machine* (Anjungan Tunai Mandiri)
BCP	: *Business Continuity Plan*
BSI	: Bank Syariah Indonesia
BSSN	: Badan Siber dan Sandi Negara
CIIP	: *Critical Information Infrastructure Protection*
CISA	: *Cybersecurity and Infrastructure Security Agency*
CSIRT	: *Computer Security Incident Response Team*
DDoS	: *Distributed Denial of Service*
DRP	: *Disaster Recovery Plan*
GCI	: *Global Cybersecurity Index*
HI	: Hubungan Internasional
IIV	: Infrastruktur Informasi Vital
ITE	: Informasi dan Transaksi Elektronik
ITU	: *International Telecommunication Union*
Kemenkominfo	: Kementerian Komunikasi dan Informatika
NSOC	: *National Security Operation Center*

PDN	: Pusat Data Nasional
PDNS	: Pusat Data Nasional Sementara
RaaS	: *Ransomware-as-a-Service*
SDM	: Sumber Daya Manusia
SLA	: *Service Level Agreement*
TNI	: Tentara Nasional Indonesia
UU PDP	: Undang-Undang Pelindungan Data Pribadi
WEF	: *World Economic Forum*

I. PENDAHULUAN

Skripsi ini menelaah analisis strategi keamanan siber Indonesia dalam menghadapi eskalasi ancaman *ransomware* transnasional pada sektor layanan publik dan perbankan periode 2020–2024. Penelitian ini krusial untuk dilakukan berdasarkan justifikasi empiris atas insiden siber pada Infrastruktur Informasi Vital (IIV), yaitu serangan *LockBit* 3.0 terhadap Bank Syariah Indonesia (2023) dan *Brain Cipher* terhadap Pusat Data Nasional Sementara (PDNS) 2 (2024). Pada latar belakang penelitian ini, peneliti membedah lanskap ancaman tersebut sebagai tantangan tata kelola data nasional yang serius di ruang siber. Analisis dilakukan dengan mengintegrasikan instrumen utama, yaitu Teori Strategi Keamanan Siber Nasional yang berlandaskan pada 5 Pilar ITU yakni aspek legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional guna mengevaluasi resiliensi infrastruktur informasi nasional. Selanjutnya, peneliti menggunakan Konsep Tata Kelola Keamanan Siber Nasional untuk mengevaluasi bagaimana tata laksana regulasi, penguatan struktur organisasi, serta pola koordinasi horizontal antar-aktor strategis dijalankan dalam merespons ancaman *ransomware*. Dalam bab ini pula, peneliti menyajikan tinjauan pustaka, rumusan masalah, tujuan penelitian, serta manfaat penelitian bagi pengembangan studi Hubungan Internasional, khususnya dalam memperkaya kajian mengenai *cyber security governance* di Indonesia.

1.1. Latar Belakang

Dalam dinamika kajian Hubungan Internasional kontemporer, sistem internasional dipahami memiliki karakteristik yang mendasar yaitu anarki, sebuah kondisi di mana tidak eksis otoritas hegemonik tunggal dunia yang mampu mengatur perilaku aktor secara absolut (Buzan et al., 1998). Seiring dengan akselerasi digitalisasi global, ruang interaksi antarnegara kini telah meluas secara masif ke dalam ranah artifisial baru yang dikenal sebagai ruang siber (*cyberspace*) (Socquet-Clerc et al., 2023). Karakteristik ruang siber yang sangat cair, asimetris, dan tanpa batas geografis yang jelas (*borderless*) telah mengaburkan batasan antara ancaman domestik dan internasional (Hansel & Silomon, 2024). Fenomena ini pada akhirnya memaksa negara-negara untuk mendefinisikan ulang konsep kedaulatan tradisional mereka ke arah kedaulatan digital, di mana kelalaian dalam membangun ketahanan siber yang kokoh (Tzavara & Vassiliadis, 2024) dapat berujung pada runtuhnya stabilitas nasional.

Pergeseran ruang interaksi ke ranah siber yang anarkis tersebut secara langsung mendisrupsi cara pandang keamanan, terutama mengenai dikotomi antara ancaman tradisional dan non-tradisional (Sunkpho et al., 2018). Jika keamanan tradisional menempatkan konfrontasi militer fisik antarnegara sebagai fokus utama, maka keamanan non-tradisional melihat bahwa ancaman di era globalisasi saat ini bersifat asimetris dan dapat diluncurkan tanpa kehadiran fisik militer (Mustikasari et al., 2025). Salah satu bentuk ancaman non-tradisional paling destruktif yang dihadapi oleh aktor negara di dunia saat ini adalah eskalasi serangan *ransomware* transnasional (Connolly et al., 2020). Dalam lanskap politik global kontemporer, ancaman *ransomware* berskala besar tidak dapat lagi dikategorikan secara sempit sebagai isu kriminalitas komputer biasa. Serangan siber jenis ini telah berevolusi menjadi sebuah tantangan politik serius yang mengancam perdamaian dan keamanan global (*threat to peace and security*) karena mampu melumpuhkan pelayanan publik serta merongrong legitimasi kedaulatan digital suatu negara (Hansel & Silomon 2024).

Di tengah struktur ruang siber yang tanpa batas yurisdiksi yang jelas tersebut, bentuk ancaman terbesar terhadap kedaulatan digital suatu negara acapkali tidak lagi bersumber dari kekuatan militer konvensional negara lain (Wibowo et al., 2024). Fokus kajian kini beralih pada pergerakan aktor non-negara transnasional (*transnational non-state actors*) yang memanfaatkan celah digital (Connolly et al. 2020). Sindikat peretas *ransomware* internasional bergerak secara dinamis melintasi yurisdiksi hukum berbagai negara guna mengeksploitasi kerentanan tata kelola sistem informasi institusi strategis (Socquet-Clerc et al., 2023). Dengan memanfaatkan anonimitas dan kemudahan model bisnis *Ransomware-as-a-Service* (RaaS), para aktor non-negara ini melancarkan enkripsi data berskala masif untuk menyandera basis data penting yang menjadi instrumen vital bagi keberlangsungan hajat hidup publik (Aggarwal, 2023). Pergeseran taktik ofensif inilah yang menempatkan ancaman asimetris dari aktor transnasional sebagai tantangan utama bagi eksistensi keamanan nasional di era kontemporer (Abrahams et al., 2024).

Melihat masifnya pergeseran taktik ofensif tersebut, penting untuk ditekankan lebih lanjut bahwa esensi dari ancaman siber ini sama sekali tidak boleh dipandang secara sempit sebagai persoalan teknis komputasi atau kegagalan baris kode pemrograman murni (Akinyemi et al., 2023). Serangan siber berbasis *ransomware* merupakan instrumen ofensif kontemporer yang menyerang jantung keamanan domestik suatu negara karena secara sengaja menargetkan kegagalan sistem pada Infrastruktur Informasi Vital (IIV) yang menopang stabilitas kehidupan publik (Mustikasari et al., 2025). Ketika pusat data strategis kementerian dan institusi keuangan penyangga ekonomi berhasil ditembus serta dikendalikan oleh aktor luar, konsekuensi dari serangan asimetris ini secara langsung melumpuhkan fungsi-fungsi kedaulatan digital dalam mengontrol keamanan informasi di dalam wilayah yurisdiksinya sendiri (Hansel & Silomon, 2024). Ketimpangan antara pertumbuhan infrastruktur digital dan kapasitas proteksi data ini menciptakan celah keamanan yang sangat rawan dieksploitasi (WEF, 2025).

Dalam konteks global yang penuh dengan kerentanan digital tersebut, Negara Indonesia memiliki posisi yang sangat strategis sekaligus rentan dalam lanskap keamanan siber global (Chotimah, 2019). Sebagai langkah responsif dalam memitigasi kerentanan tata kelola siber domestik yang rawan dieksploitasi tersebut, Pemerintah Indonesia sepanjang rentang tahun 2020 hingga 2024 mulai menginisiasi penguatan instrumen kebijakan siber secara intensif (Sunkpho et al., 2018). Urgensi penguatan ini berakar pada kebutuhan mendesak untuk membangun kerangka kerja institusional yang lebih kokoh di bawah komando Badan Siber dan Sandi Negara (BSSN) guna menghadapi ancaman non-militer yang terus berevolusi. Periode tersebut menjadi momentum krusial bagi negara dalam melahirkan berbagai produk hukum baru dan standarisasi tata kelola digital untuk menciptakan daya tangkal siber domestik yang integratif (Socquet-Clerc et al., 2023).

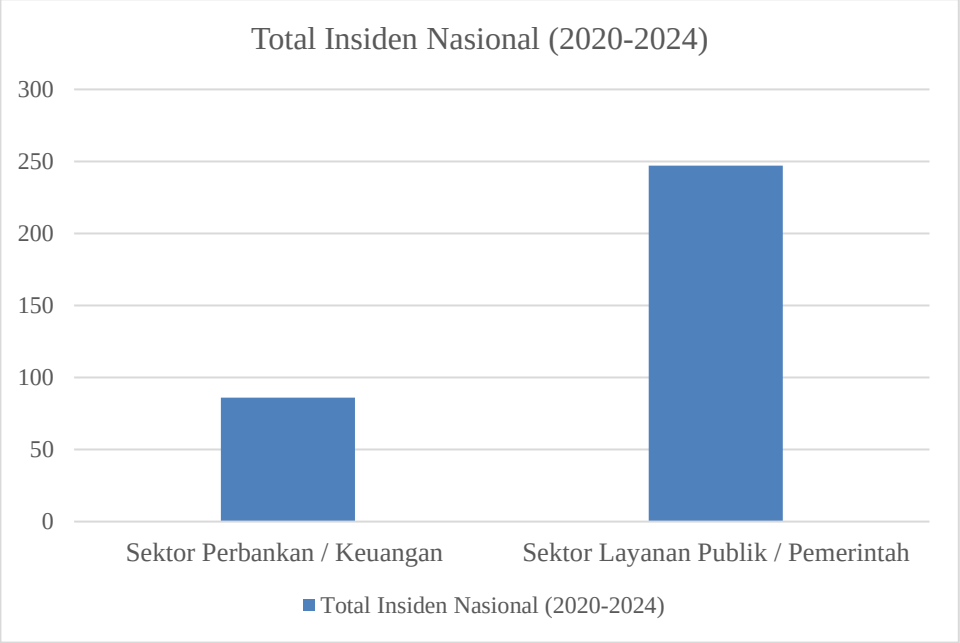
Manifestasi nyata dari komitmen institusional negara dalam merumuskan regulasi strategis tersebut ditandai dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional (Perpres SKSN) (Sunkpho et al., 2018). Dalam tinjauan hukum dan tata kelola siber domestik, kehadiran instrumen hukum tertulis (*legal measures*) ini secara teoretis dibentuk oleh negara untuk mengikat para pengendali data agar menerapkan standarisasi keamanan yang ketat guna meminimalisir risiko kebocoran data nasional (Socquet-Clerc et al., 2023). Melalui regulasi ini, Pemerintah Indonesia berusaha memaksakan kepatuhan teknis (*compliance*) di tingkat domestik agar memiliki daya tahan yang lebih solid ketika berhadapan dengan penetrasi ofensif dari jaringan peretas eksternal di ruang siber (Abrahams et al., 2024).

Keberadaan berbagai produk hukum dan instrumen kebijakan siber yang lahir sepanjang era 2020–2024 tersebut sayangnya memicu tanda tanya besar ketika dihadapkan pada fakta empiris di lapangan. Meskipun secara normatif otoritas negara telah memiliki panduan strategi keamanan siber, realitasnya Indonesia justru mengalami serangkaian insiden serangan siber terbesar dalam sejarahnya pada kurun

waktu 2023 hingga 2024. Krisis siber berturut-turut yang menghantam sektor publik maupun privat ini membuktikan adanya celah kepatuhan teknis (*compliance gap*) yang menganga antara regulasi tertulis dengan implementasi riil di dunia nyata. Dinamika ini memperlihatkan bahwa keberadaan hukum normatif tidak serta-merta linear dengan kesiapan taktis operasional dan tingkat kematangan tata kelola keamanan siber di lapangan.

Hantaman nyata dari kegagalan taktis tersebut terwujud secara dramatis pada Mei 2023 ketika sektor perbankan strategis nasional menjadi target utama operasi ofensif. Kelompok peretas non-negara transnasional yang dikenal sebagai *LockBit* 3.0 meluncurkan serangan siber asimetris berbasis *ransomware* yang berhasil menembus dan menyandera seluruh inti sistem operasional Bank Syariah Indonesia (BSI) (Akinyemi et al., 2023). Tidak berhenti di situ, eskalasi ancaman mencapai titik puncaknya pada Juni 2024 ketika sektor administrasi pemerintahan publik lumpuh total akibat serangan *ransomware* varian *Brain Cipher* terhadap Pusat Data Nasional Sementara 2 (PDNS 2) di Surabaya (Mustikasari et al., 2025). Fenomena konfrontasi siber asimetris yang melanda BSI dan PDNS 2 merupakan representasi dari eskalasi krisis keamanan siber yang jauh lebih luas di tingkat makro nasional (Mustikasari et al., 2025). Guna memetakan posisi strategis antara tren ancaman berskala nasional dengan batasan objek studi kasus yang diangkat dalam penelitian ini, dapat dilihat melalui grafik perbandingan berikut:

Gambar 1. 1 Jumlah Insiden Serangan Ransomware (2020-2024)



Sumber: Laporan Tahunan Monitoring Keamanan Siber BSSN (2020–2024), Dokumen Investigasi Insiden BSI & PDNS 2, diolah oleh Peneliti (2026).

Berdasarkan visualisasi pada Grafik 1.1, data tersebut memperjelas adanya kesenjangan kuantitatif yang nyata antara realitas makro nasional dengan pembatasan studi kasus yang peneliti lakukan. Sepanjang kurun waktu 2020–2024, Indonesia secara agregat mencatatkan total 86 insiden ransomware besar di sektor perbankan/keuangan serta 247 insiden di sektor layanan publik/pemerintah. Kendati demikian, pemilihan BSI (2023) dan PDNS 2 (2024) sebagai objek amatan didasarkan pada argumen bahwa kedua insiden ini merupakan representasi puncak kehancuran tata kelola siber yang melumpuhkan kedaulatan data dan merugikan jutaan hajat hidup warga sipil secara sistemik (Hansel & Silomon, 2024). Sebagai bentuk justifikasi empiris atas kompleksitas dan besarnya parameter dampak kehancuran tersebut, visualisasi ringkasnya disajikan melalui tabel berikut:

Tabel 1. 1 Rekapitulasi Data Empiris Dampak Serangan Ransomware Transnasional di Indonesia (2020–2024)

No	Parameter Data / Kasus	Indikator Kuantitatif	Dampak Struktural / Sistemik	Sumber Resmi
1.	Trafik Anomali Siber Nasional	> 1 Miliar anomali per tahun.	Tingginya tingkat kerentanan perimeter ruang digital domestik.	Laporan Tahunan BSSN (2023)
2.	Kasus Bank Syariah Indonesia (BSI) - 2023	1,5 Terabyte (TB) data dieksfiltrasi.	Kelumpuhan sistem ATM & *Mobile Banking* selama 5 hari berturut-turut.	BSSN & Kominfo (2023)
3.	Kasus Pusat Data Nasional Sementara 2 - 2024	282 Instansi Pemerintah lumpuh.	Kelumpuhan total layanan publik (Imigrasi, Beasiswa, dll) berminggu-minggu.	Kemenkominfo & DPR RI (2024)
4.	Tingkat Kepatuhan Cadangan Data (*Backup*)	Hanya 2% dari 282 Instansi.	Terjadinya *governance failure* akibat minimnya	Transkrip Raker DPR (2024)

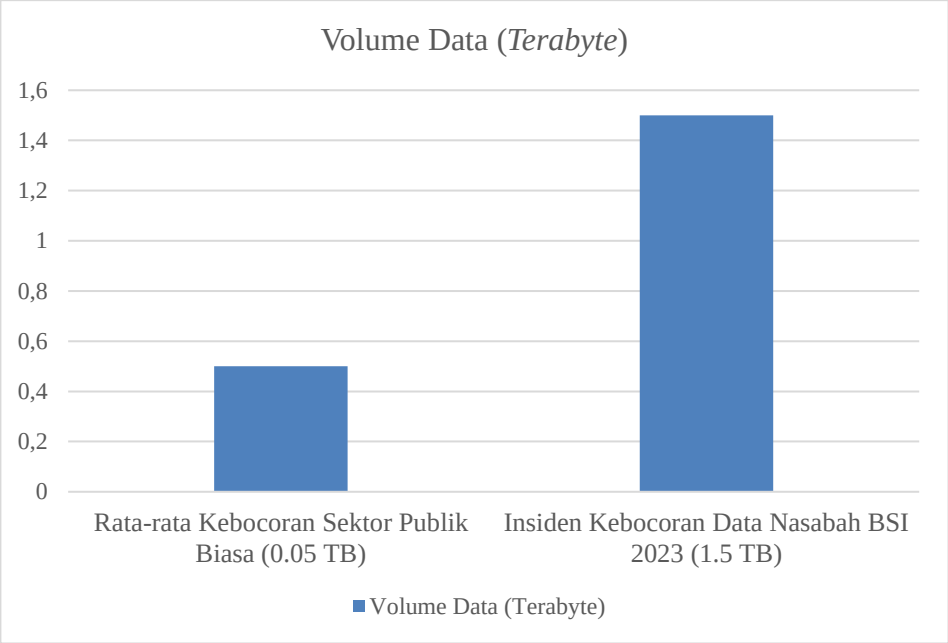
			infrastruktur replikasi data.	

Sumber: Laporan Tahunan Monitoring Keamanan Siber BSSN (2020–2024), Laporan Insiden BSI (2023), & Dokumen Investigasi PDNS 2 (2024); diolah oleh Peneliti (2026).

Melalui pemaparan Tabel 1.1, dapat dianalisis bahwa parameter kerugian material dan non-material akibat infiltrasi siber transnasional di Indonesia telah menuntut adanya evaluasi total terhadap model pengamanan yang ada. Lonjakan trafik anomali nasional yang menembus angka 1 miliar per tahun membuktikan ruang digital Indonesia terus dibombardir oleh eksploitasi peretas eksternal. Ketika pertahanan hulu ini lumpuh, dampaknya langsung merembet pada eksfiltrasi data korporasi vital serta berhentinya fungsi birokrasi negara (Akinyemi et al., 2023). Hal ini mengonfirmasi teori bahwa di era kontemporer, serangan ransomware tidak sekadar memeras secara finansial, melainkan berwujud operasi sabotase yang melumpuhkan kapasitas fungsional sebuah negara berdaulat.

Dampak kerusakan yang paling masif mencederai sektor finansial ini bermanifestasi pada rapuhnya pilar teknis dan organisasi dalam kerangka strategi keamanan siber nasional, yang pada tingkat operasional memicu kegagalan tata kelola (*governance failure*) yang fatal (Krahmann, 2003). Serangan *ransomware* oleh sindikat transnasional *LockBit* 3.0 terhadap server Bank Syariah Indonesia (BSI) pada Mei 2023 menjadi bukti empiris mengenai adanya kesenjangan kepatuhan (*compliance gap*) yang nyata terhadap regulasi manajemen risiko siber pada lembaga keuangan pelindung aset publik . Untuk mengamati visualisasi volume data sensitif nasabah yang berhasil ditarik secara ilegal oleh peretas transnasional tersebut ke jaringan internet gelap (*dark web*), dapat dicermati melalui grafik di bawah ini:

Gambar 1. 2 Grafik Volume Eksfiltrasi Data Kasus BSI (2023)



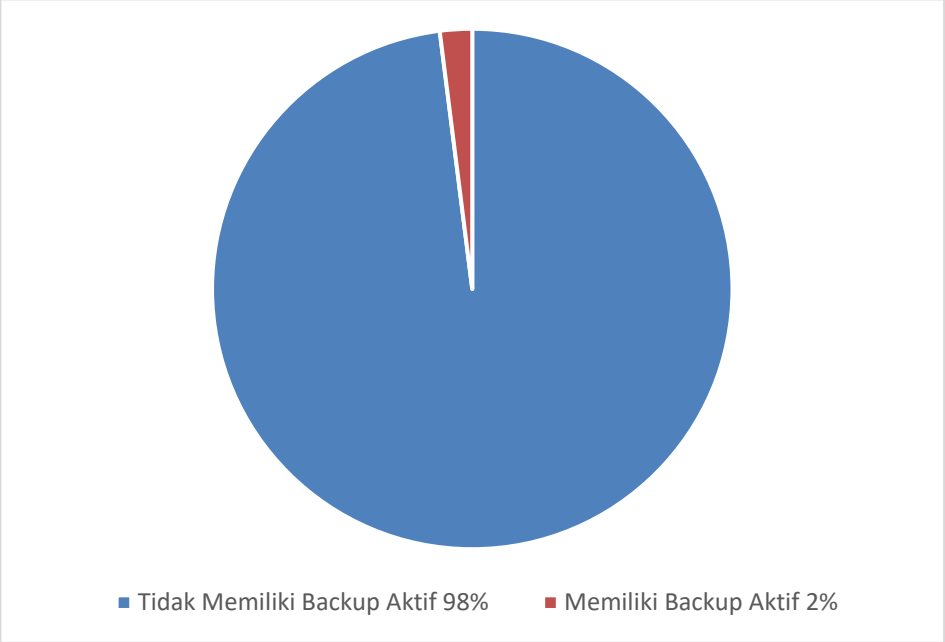
Sumber: Keterangan Resmi BSSN, Laporan Keterbukaan Informasi BSI (2023); diolah oleh Peneliti (2026).

Sebagaimana dipaparkan pada Grafik 1.2, volume kebocoran data yang dialami BSI menembus angka ekstrem sebesar 1,5 *Terabyte* (TB). Angka ini melompat sangat tinggi jika dibandingkan dengan rata-rata insiden kebocoran data publik biasa yang umumnya berhasil diisolasi di bawah kisaran 0,05 TB. Eksfiltrasi raksasa yang mencakup rekam jejak finansial, data pribadi karyawan, hingga informasi sensitif jutaan nasabah ini menjadi bukti empiris terjadinya kesenjangan kepatuhan teknis instansi perbankan terhadap regulasi UU PDP No. 27 Tahun 2022 (Kholis, 2024). Kerugian non-material berupa runtuhnya reputasi institusi perbankan syariah terbesar di Indonesia ini mengespos kelemahan fundamental tata kelola risiko siber korporasi vital di mata dunia internasional (WEF, 2025).

Tidak berhenti pada sektor perbankan privat, eskalasi ancaman siber mencapai titik kulminasinya pada pertengahan tahun 2024 ketika sektor administrasi

pemerintahan publik lumpuh total. Pusat Data Nasional Sementara 2 (PDNS 2) di Surabaya sebagai infrastruktur tunggal penampung integrasi data kementerian, menjadi sasaran ofensif dari varian ransomware baru bernama *Brain Cipher* (Simorangkir et al., 2024). Serangan asimetris ini melampaui skala infiltrasi biasa karena sanggup mengunci dan menyandera enkripsi basis data milik lebih dari 280 instansi pemerintah pusat dan daerah (Simorangkir et al., 2024).

Gambar 1. 3 Grafik Kesenjangan Kepatuhan (Compliance Gap) Pengaktifan Replikasi Cadangan Data Instansi Pemerintah pada Infrastruktur PDNS 2



Sumber: Laporan Investigasi Insiden PDNS 2 BSSN-Kominfo; diolah oleh Peneliti (2026).

Pembagian persentase pada Grafik 1.3 menyingkap fakta memprihatinkan bahwa kegagalan penanganan darurat siber nasional dipicu oleh kesenjangan kepatuhan (*compliance gap*) yang sangat fatal (Abrahams et al. 2024). Pasca-insiden, audit BSSN mengungkap bahwa 98% instansi pemerintah pengguna (276 instansi) tidak mengaktifkan sistem replikasi cadangan (*backup*) data fungsional. Sebaliknya,

hanya ada 2% instansi yang memiliki data cadangan terisolasi di Pusat Data kedua Batam. Data kuantitatif ini membuktikan bahwa kebijakan tata laksana mitigasi risiko siber yang diamanatkan dalam Perpres SKSN No. 47 Tahun 2023 diabaikan di tataran praktis birokrasi, sehingga saat Brain Cipher melumpuhkan server utama, fungsi pelayanan publik sipil terhenti total akibat ketiadaan redundansi data.

Kegagalan dalam mempertahankan pilar keamanan siber tersebut pada akhirnya memicu urgensi teoretis yang mendalam mengenai pentingnya tata kelola resiliensi siber nasional dalam kajian Hubungan Internasional (Tzavara & Vassiliadis, 2024). Perlindungan terhadap aset strategis negara tidak lagi cukup jika hanya bersandar pada instrumen hukum normatif tertulis di atas kertas tanpa dibarengi kapabilitas operasional yang terintegrasi di lapangan. Implementasi kebijakan yang bertumpu pada dimensi tata kelola (*cybersecurity governance*) menekankan pentingnya komando tersentralisasi untuk menghapus tumpang tindih sektoral antarinstansi pemerintah (Socquet-Clerc et al., 2023). Ketiadaan keselarasan ini akan membuat mata rantai respon domestik menjadi sangat lamban, permisif terhadap kelalaian, dan selamanya rapuh menghadapi penetrasi canggih dari jaringan aktor luar negeri.

Urgensi untuk menganalisis tata kelola keamanan siber nasional secara menyeluruh inilah yang menempatkan studi ini pada posisi krusial dalam dinamika kajian Hubungan Internasional (Buzan et al., 1998). Upaya Negara Indonesia dalam membangun kapasitas keamanan siber tidak boleh lagi ditunda mengingat taruhannya adalah eksistensi kedaulatan digital di tengah ketidakpastian politik global (Hansel & Silomon, 2024). Maka dari itu, optimalisasi kebijakan siber nasional melalui penataan simultan terhadap lima pilar utama Strategi Keamanan Siber Nasional standar Uni Telekomunikasi Internasional yang mencakup pilar tindakan hukum (*legal measures*), tindakan teknis (*technical measures*), tata kelembagaan (*organizational measures*), peningkatan kapasitas SDM (*capacity building*), serta jaringan kerja sama (*cooperation*) harus dipandang sebagai satu kesatuan strategi pertahanan non-militer

yang utuh demi melindungi Infrastruktur Informasi Vital dari ancaman infiltrasi aktor transnasional (Socquet-Clerc et al., 2023).

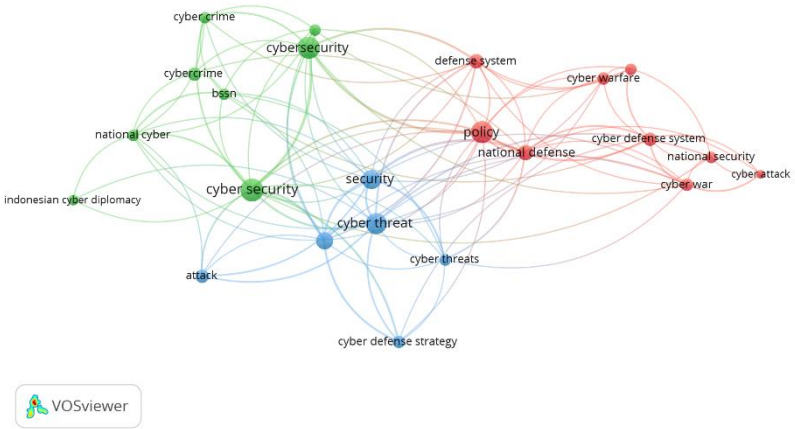
1.2. Penelitian Terdahulu

Dalam menyusun penelitian ini, peneliti menggunakan beberapa penelitian terdahulu dalam membentuk sebuah kerangka pemikiran, termasuk dalam menentukan konsep atau teori yang akan peneliti gunakan dalam meneliti kasus ini. Secara spesifik, penelitian yang menekankan pada strategi keamanan siber Indonesia dalam menangani serangan *ransomware* secara komprehensif termasuk belum banyak dilakukan. Meski demikian, penelitian lainnya yang bersinggungan dengan topik ini telah cukup banyak dilakukan oleh para akademisi dari berbagai disiplin ilmu.

Dalam memetakan perkembangan studi terkait, peneliti melakukan penelusuran literatur secara sistematis melalui basis data *Google Scholar* yang diindeks menggunakan *Publish or Perish*. Parameter pencarian ditetapkan pada periode 2020–2024 dengan batasan hasil pencarian maksimal 200 judul. Setelah melalui proses seleksi yang ketat dengan mengutamakan keterkaitan langsung terhadap isu *ransomware* dan strategi keamanan siber, terpilih 15 artikel jurnal utama. Artikel-artikel tersebut selanjutnya dikelompokkan berdasarkan kecenderungan fokus analisisnya, di mana penelitian-penelitian tersebut menekankan pada, strategi keamanan siber nasional dan penguatan peran BSSN dalam menjaga kedaulatan data dan infrastruktur informasi vital (Ikhssani et al., 2024; Makbul and Ismail, 2023; Budi et al., 2021; Wardana et al., 2022; Witjaksono and Kriswibowo, 2023) ; analisis implementasi kebijakan hukum dan tata kelola keamanan siber khususnya terkait perlindungan data pribadi dan penegakan hukum (Tobondo et al., 2024; Najwa, 2024; Rahakbauw and Batubara, 2024; Amarullah et al., 2021); serta mitigasi ancaman spesifik seperti *ransomware* dan kebocoran data yang menyerang sektor kritis maupun data publik (Sutikno & Stiawan, 2022; Sawlani & Supriyadi, 2024; Dyahtaryani & Trianto, 2024; Dwiaji et al., 2024; Srilaksmi et al., 2023; Yuniarti et al., 2023)

Untuk membuktikan *novelty* tersebut, peneliti menggunakan metode bibliometrik dengan menggunakan perangkat lunak seperti Publish or Perish untuk mendapatkan basis data dan VOSviewer untuk memetakan hasil penelitian. Bibliometrik adalah penggunaan metode statistik untuk menganalisis buku, artikel, dan publikasi lainnya, terutama yang berkaitan dengan konten ilmiah. Peneliti dapat menggunakan kata kunci seperti *"cyber defense Indonesia," "ransomware attack Indonesia," ”cyber attack", “cybersecurity strategy," dan "BSSN"*. Dengan menggunakan kata kunci tersebut, peneliti dapat menemukan sumber terkait dan memetakan hasil penelitian yang ada. Dari basis data yang diperoleh, yang kemudian dipetakan oleh VOSviewer, peneliti dapat menemukan minimnya penelitian yang secara spesifik berfokus pada topik ini, sehingga peneliti dapat memfokuskan analisisnya pada strategi keamanan siber Indonesia dalam menangani serangan *ransomware*. Berikut hasil pemetaan VOSviewer yang dilakukan oleh peneliti:

Gambar 1. 4 Hasil Pemetaan VosViewer peneliti



Sumber: diolah oleh peneliti untuk keperluan penelitian

Penelitian pertama adalah studi yang dilakukan oleh Wiwik Mustikasari, Ahmad G. Dohamid, dan Fauzia G. Cempaka dalam artikel mereka yang berjudul Strategi Pertahanan Non Konvensional Indonesia dalam Menangkal Ancaman Siber Asimetris: Studi Kasus Serangan terhadap Infrastruktur Kritis (Mustikasari et al., 2025). Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis secara mendalam strategi pertahanan non-konvensional yang diterapkan oleh Indonesia dalam menghadapi ancaman siber asimetris yang semakin kompleks. Data penelitian ini bersumber dari data sekunder yang komprehensif, yang diperoleh melalui studi literatur, dokumen-dokumen resmi pemerintah, dan laporan-laporan terkait pertahanan siber. Penelitian ini menggunakan konsep pertahanan siber dan manajemen risiko sebagai kerangka analisisnya. Tujuan utama dari penelitian ini ialah untuk memberikan jawaban atas pertanyaan mengenai efektivitas strategi yang telah ada dan memberikan gambaran mengenai tantangan yang masih menghambat, terutama dalam hal koordinasi antar lembaga dan peningkatan kesadaran masyarakat terhadap ancaman ransomware dan serangan siber lainnya.

Penelitian kedua adalah studi yang dilakukan oleh Arinaldo Adma, Yusuf Marsel Surbakti, dan Puspita Sari dalam artikelnya yang berjudul Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan (Adma et al., 2023). Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis deskriptif untuk mengkaji secara sistematis transformasi yang diperlukan dalam sistem pertahanan siber Indonesia. Data dari penelitian ini bersumber dari data sekunder yang dikumpulkan dari berbagai laporan, berita, dan jurnal ilmiah yang relevan. Penelitian ini menggunakan konsep keamanan siber dan transformasi sistem sebagai kerangka teoritisnya. Tujuan utama dari penelitian ini ialah untuk menunjukkan bahwa penanganan siber merupakan salah satu aspek pertahanan keamanan yang sangat penting di era digital saat ini, serta mengidentifikasi langkah-langkah konkret yang harus diambil untuk mencapai kemandirian siber, seperti penguatan kapasitas talenta digital dan kolaborasi antarpihak.

Penelitian ketiga adalah studi yang dilakukan oleh Y. C. Mahendra dan N. K. D. S. A. Pinatih dalam artikelnya yang berjudul Strategi Penanganan Keamanan Siber (*Cyber Security*) Di Indonesia (Pinatih et al., 2023). Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur guna menganalisis berbagai strategi penanganan keamanan siber yang telah ada di Indonesia. Data dari penelitian ini bersumber dari data sekunder yang diperoleh dari berbagai jurnal ilmiah, artikel, dan laporan penelitian yang relevan dengan keamanan siber. Penelitian ini menggunakan konsep strategi keamanan siber dan tipologi ancaman siber sebagai landasan analisisnya. Tujuan utama dari penelitian ini ialah untuk membahas tantangan dan strategi yang dihadapi Indonesia dalam implementasi keamanan siber, dengan fokus pada bagaimana mengatasi serangan ransomware dan pencurian data pribadi yang semakin marak terjadi di sektor publik maupun swasta.

Penelitian keempat adalah studi yang dilakukan oleh Yusep Ginanjar dalam artikelnya yang berjudul Strategi Indonesia Membentuk *Cyber Security.* Dalam Menghadapi Ancaman *Cyber Crime* Melalui Badan Siber Dan Sandi Negara (Ginanjar, 2022). Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis strategi yang diimplementasikan oleh Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman kejahatan siber yang terus berkembang. Data dari penelitian ini bersumber dari data sekunder yang diperoleh dari publikasi BSSN, laporan pemerintah, dan berbagai jurnal terkait. Penelitian ini menggunakan konsep strategi *cyber security* dan lima pilar *Global Cybersecurity Index* (GCI) sebagai kerangka pemikirannya. Tujuan utama dari penelitian ini ialah untuk menganalisis strategi yang diimplementasikan BSSN dalam membentuk keamanan siber, serta menyoroti tantangan yang dihadapi dalam mengatasi ancaman yang semakin masif, terutama terhadap infrastruktur vital.

Penelitian kelima adalah studi yang dilakukan oleh Muhamad Rizki Hapizon dalam skripsinya yang berjudul Analisis Kerjasama *Cyber Security* Indonesia-Australia dalam Menangani Kejahatan Siber di Indonesia (Hapizon & Rizki, 2023). Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus komparatif untuk menganalisis kerja sama bilateral antara Indonesia dan Australia.

Data dari penelitian ini bersumber dari data sekunder yang diperoleh dari dokumen kerja sama, laporan pemerintah, dan artikel berita. Penelitian ini menggunakan konsep kerja sama internasional dan diplomasi siber sebagai landasan analisisnya. Tujuan utama dari penelitian ini ialah untuk menganalisis bentuk kerja sama yang dilakukan oleh kedua negara dalam menangani kejahatan siber dan mengidentifikasi seberapa efektif kerja sama tersebut dalam meminimalisir tingkat kejahatan siber, termasuk serangan *ransomware* yang merugikan pertahanan dan ekonomi kedua negara.

Penelitian-penelitian tersebut memiliki kesamaan pendekatan dan metode yang akan peneliti gunakan dalam penelitian ini, yaitu penelitian kualitatif dengan metode deskriptif. Penelitian yang peneliti lakukan di sini tentu berbeda dengan penelitian-penelitian terdahulu dalam hal substansi dan fokus analisis. Dalam penelitian ini, peneliti akan memberikan gambaran mendalam mengenai respons Indonesia menggunakan lensa Teori Strategi Keamanan Siber Nasional dan Konsep Tata Kelola Keamanan Siber Nasional, guna memberikan kejelasan mengenai bagaimana negara mengelola koordinasi horizontal lintas aktor dalam memitigasi risiko data pada Infrastruktur Informasi Vital (IIV). Peneliti juga akan menyajikan data dan fakta terbaru terkait insiden serangan *ransomware* pada infrastruktur kritis nasional periode 2020–2024, yang tentunya bersumber dari sumber yang kredibel dan terbaru, untuk menciptakan kebaruan informasi dan data dalam studi Hubungan Internasional.

1.3. Rumusan Masalah

Sepanjang tahun 2023 hingga 2024, serangkaian serangan *ransomware* berskala besar melumpuhkan Infrastruktur Informasi Vital (IIV) Indonesia, di mana kelompok peretas transnasional *LockBit* 3.0 berhasil menyandera sistem Bank Syariah Indonesia (2023) dan varian *Brain Cipher* melumpuhkan Pusat Data Nasional Sementara (PDNS) 2 Surabaya (2024). Serangan asimetris ini melampaui batas kriminalitas digital biasa karena secara nyata merusak resiliensi infrastruktur informasi serta menghentikan ratusan layanan publik yang krusial bagi kehidupan bernegara.

Fenomena krisis ini menarik perhatian besar mengenai rentannya ketahanan domestik dan membuktikan adanya celah yang nyata dalam implementasi 5 Pilar Strategi Keamanan Siber ITU yakni pilar legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional yang belum mampu beroperasi secara optimal dalam membendung ancaman tersebut. Pada akhirnya, situasi ini memicu krisis kedaulatan digital nasional dan memaksa Indonesia untuk mengevaluasi kembali Konsep Tata Kelola Keamanan Siber Nasional-nya, terutama dalam aspek sinkronisasi regulasi, pola koordinasi horizontal antar-aktor strategis, serta implementasi penguatan struktur organisasi keamanan siber dalam menghadapi aktor non-negara transnasional yang memiliki kapabilitas siber yang canggih.

Berdasarkan rumusan masalah yang telah diuraikan di atas, penulis merumuskan masalah sebagai berikut:

"Bagaimana strategi keamanan siber Indonesia dalam menghadapi ancaman ransomware tersebut?"

1.4. Tujuan Penelitian

1. Menjelaskan kebijakan Strategi Keamanan Siber Nasional Indonesia dalam menghadapi ancaman *ransomware* transnasional periode 2020–2024 berdasarkan pilar-pilar strategis ITU.
2. Menjelaskan hambatan regulasi dan koordinasi kelembagaan dalam Tata Kelola Keamanan Siber (*Cybersecurity Governance*) Indonesia melalui studi kasus serangan pada Bank Syariah Indonesia (2023) dan Pusat Data Nasional Sementara 2 (2024).

1.5. Manfaat Penelitian

Penelitian ini diharapkan mampu memberi manfaat, antara lain:

a. Manfaat Akademis**:** Peneliti berharap hasil penelitian ini mampu berkontribusi bagi kajian-kajian dalam Ilmu Hubungan Internasional, utamanya dalam ranah keamanan non-tradisional, strategi keamanan nasional, serta diskursus keamanan siber. Penelitian ini diharapkan dapat memperkaya literatur akademik mengenai strategi keamanan siber suatu negara dalam menghadapi ancaman dari aktor eksternal, sekaligus menjembatani celah kajian (gap) mengenai tata kelola keamanan siber dari kacamata Hubungan Internasional. Peneliti juga berharap hasil penelitian ini dapat menjadi referensi atau inspirasi bagi peneliti lain dalam mengembangkan topik serupa, khususnya terkait penerapan postur keamanan siber di negara-negara berkembang di kawasan Asia Tenggara.
b. Manfaat Praktis: Secara praktis, peneliti berharap hasil penelitian ini dapat menjadi media pembelajaran dan sumber wawasan yang komprehensif, tidak hanya bagi kalangan akademisi Hubungan Internasional, tetapi juga bagi para pembuat kebijakan, praktisi keamanan siber, dan masyarakat luas. Penelitian ini diharapkan mampu menjadi bahan evaluasi dan rujukan strategis bagi lembaga-lembaga pemangku kepentingan seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Pertahanan, beserta entitas operator infrastruktur kritis lainnya. Hal ini ditujukan agar proses perumusan regulasi tata kelola keamanan dan penyusunan strategi keamanan siber Indonesia dapat berjalan lebih sinergis dan efektif dalam meredam eskalasi ancaman *ransomware* dari aktor eksternal di masa mendatang.

II. TINJAUAN PUSTAKA

Bab ini akan menyajikan tinjauan pustaka yang terbagi ke dalam dua bagian. Setelah menguraikan landasan konseptual yang terdiri dari konsep Tata Kelola Keamanan Siber *(Cyber Security Governance)*, dan Teori Strategi Keamanan Siber Nasional (*National Cybersecurity Strategy*), pada bagian kedua akan dipaparkan kerangka pemikiran yang bertujuan untuk menciptakan alur pikir yang diterapkan dalam penelitian ini serta memberikan gambaran mengenai strategi keamanan siber yang dilakukan oleh Indonesia dalam berupaya menangani serangan ransomware dari periode tahun 2020 hingga 2024.

2.1. Landasan Konseptual

Konsep serta teori yang digunakan oleh peneliti dalam landasan konseptual tentunya menjadi modal bagi peneliti dalam membingkai kerangka analisis dalam penelitian ini. Adapun poin-poin dalam landasan ini mengintegrasikan Teori Strategi Keamanan Siber Nasional, yang dalam implementasinya dijabarkan melalui 5 Pilar Strategi Keamanan Siber ITU (*International Telecommunication Union's Cybersecurity Strategy Pillars*) mencakup aspek legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional sebagai instrumen utama untuk membedah langkah strategis pemerintah dalam merespons ancaman *ransomware*. Selain itu, peneliti menggunakan Konsep Tata Kelola Keamanan Siber Nasional sebagai pisau analisis untuk memahami bagaimana pola koordinasi horizontal antar-aktor strategis, sinkronisasi regulasi, serta efektivitas struktur organisasi

dijalankan di lapangan saat menghadapi ancaman transnasional yang secara langsung mengganggu stabilitas data publik. Peneliti juga akan menjelaskan prinsip-prinsip dasar kematangan siber yang menjadi fondasi dalam menjaga resiliensi infrastruktur informasi negara sesuai dengan standar yang ditetapkan oleh ITU. Untuk memberikan gambaran terkait dinamika serangan siber kontemporer, peneliti akan menjabarkan karakteristik *ransomware* dalam mengeksploitasi celah kerentanan sistem pada infrastruktur informasi vital domestik melalui pendekatan manajemen risiko yang komprehensif, dengan mempertimbangkan tantangan dalam setiap pilar strategi siber yang telah ditetapkan.

2.1.1. Konsep Tata Kelola Keamanan Siber (*Cyber Security Governance*)

Dalam mengkaji respons kebijakan Pemerintah Indonesia terhadap eskalasi ancaman siber kontemporer, penerapan Teori Strategi Keamanan Siber Nasional memerlukan dukungan analitis yang lebih spesifik melalui aplikasi Konsep Tata Kelola Keamanan Siber (*Cybersecurity Governance*). Konsep ini hadir sebagai kacamata analitis yang krusial dalam studi Hubungan Internasional untuk memahami bahwa struktur keamanan kontemporer tidak lagi bergerak secara hierarkis-sentralistik di bawah kendali tunggal militer, melainkan telah bergeser menuju pola interaksi yang bersifat fragmentatif, kompleks, dan melibatkan banyak aktor (*multi-stakeholder*). Sebagaimana diargumenkan dalam fondasi konseptual oleh (Krahmann, 2003), pasca-Berakhirnya Perang Dingin, konsep keamanan telah mengalami perluasan makna dari yang semula berpusat pada ancaman militer antarnegara (*state-centric*) menjadi perlindungan terhadap masyarakat digital dan fungsionalitas sistem secara luas.

Pergeseran paradigma ini memicu lahirnya tatanan tata laksana keamanan baru di mana pengoordinasian, pengelolaan, dan regulasi atas risiko tidak lagi menjadi monopoli absolut dari lembaga pertahanan konvensional, melainkan melibatkan pembagian otoritas yang tersebar antara lembaga sipil pemerintah, korporasi swasta,

hingga penyedia infrastruktur digital. Perubahan lanskap keamanan digital ini menuntut negara untuk tidak lagi memandang kedaulatan hanya dari batas-batas teritorial fisik di darat, laut, dan udara. Menurut pemikiran (Krahmann, 2003), aktor-aktor swasta dan penyedia layanan teknologi informasi kini memiliki pengaruh yang sangat besar dalam menentukan tingkat kerentanan atau resiliensi pertahanan siber suatu negara. Maka dari itu, konsep tata kelola keamanan siber memfasilitasi peneliti untuk melihat sejauh mana interaksi dan pembagian peran (*functional differentiation*) antara institusi pemerintah dan aktor non-negara terjalin dalam meredam ancaman.

Dalam konteks Hubungan Internasional, model tata kelola ini bergeser dari bentuk *government* yang kaku dan tersentralisasi menuju bentuk *governance* yang lebih fleksibel, di mana koordinasi horizontal menjadi kunci utama untuk merumuskan kebijakan pertahanan non-kinetik yang inklusif terhadap ancaman siber. Pengembangan lebih lanjut mengenai karakteristik tata kelola keamanan ini dijabarkan secara komprehensif oleh Webber, Croft, Howorth, Terriff, dan Krahmann (2004). Mereka menegaskan bahwa *security governance* merupakan instrumen analitis yang tepat untuk membedah bagaimana aturan, norma, institusi, dan pola koordinasi bekerja secara kolektif dalam memproduksi keamanan di tengah situasi anarki ruang siber. Tata kelola keamanan siber nasional tidak sekadar membahas soal pengadaan teknologi enkripsi atau penguatan perangkat keras secara terpisah, melainkan menyoroti bagaimana instansi-instansi negara menafsirkan karakteristik ancaman seperti eskalasi serangan *ransomware* transnasional dan mengartikulasikannya ke dalam tindakan kebijakan kolektif.

Melalui pendekatan tata kelola ini, fokus analisis diarahkan pada bagaimana sebuah negara mengoordinasikan tatanan institusionalnya agar mampu meredam konflik ego sektoral, menegakkan aturan kepatuhan (*regulatory compliance*), serta menjamin keberlangsungan fungsi layanan publik vital saat terjadi krisis siber berskala besar. Lebih jauh lagi, (Webber et al., 2004) menekankan bahwa legitimasi dan efektivitas dari suatu sistem tata kelola keamanan diukur dari kemampuannya untuk mengikat institusi-institusi di dalamnya agar mematuhi aturan (*rules of game*) yang

telah disepakati bersama. Dalam ruang siber yang tidak memiliki batas geografis, ancaman seperti *ransomware* bekerja melampaui batas kedaulatan negara konvensional dan mengeksploitasi kelengahan birokrasi domestik. Tata kelola keamanan siber yang rapuh ditandai dengan ketidakmampuan instansi-instansi negara untuk menyelaraskan kebijakan penanganan insiden siber, yang mana aturan pengamanan sering kali diabaikan oleh lembaga pengelola data di tingkat praktis.

Ketika konsep tata kelola keamanan siber ini diturunkan dan dikontekstualisasikan ke dalam dinamika domestik di Indonesia, secara mendalam mengenai urgensi penataan kelembagaan nasional melalui pembentukan institusi khusus yang memegang mandat tersentralisasi, yaitu Badan Siber dan Sandi Negara (BSSN) (Chotimah, 2019). Konsep *cybersecurity governance* dalam ruang lingkup nasional Indonesia menekankan pentingnya kehadiran arsitektur kelembagaan resmi yang kuat untuk mengintegrasikan tata kelola keamanan siber domestik sekaligus menjalankan fungsi pertahanan siber yang protektif terhadap kepentingan nasional. Kedaulatan siber suatu negara di abad ke-21 tidak hanya ditentukan oleh kepemilikan alutsista militer fisik, melainkan dari kapasitas institusi nasionalnya dalam menetapkan standarisasi manajemen risiko siber, mengawasi kepatuhan lembaga pengelola data publik, serta mengoordinasikan langkah mitigasi insiden siber secara cepat dan responsif lintas sektoral.

Dalam pandangan (Chotimah 2019), tata kelola keamanan siber nasional yang tangguh juga memiliki korelasi langsung dengan kapabilitas negara dalam menjalankan diplomasi siber di ranah global. Mengingat aktor peretas *ransomware* transnasional kerap beroperasi dari luar yurisdiksi hukum Indonesia, BSSN selaku aktor sentral dalam *cybersecurity governance* di Indonesia dituntut untuk mampu membangun jaringan kerja sama internasional, baik secara bilateral maupun multilateral. Penataan tata kelola di tingkat domestik harus menjadi cerminan dari kesiapan negara untuk terlibat dalam pertukaran intelijen ancaman (*threat intelligence*) dan penyelarasan norma hukum siber global. Akibatnya, kekokohan hubungan koordinasi horizontal-koordinatif antarlembaga di dalam negeri menjadi prasyarat mutlak yang melandasi

implementasi posisi diplomasi siber Indonesia saat berhadapan dengan ekosistem ancaman siber internasional.

Urgensi penataan tata kelola keamanan siber yang komprehensif bagi kelangsungan kedaulatan digital ini juga sejalan dengan kajian pembangunan masyarakat digital. Dalam konteks global bahwa adopsi teknologi informasi dan pemutakhiran sistem digital berskala nasional di negara-negara berkembang harus diimbangi dengan kesiapan tata kelola keamanan siber domestik yang matang guna melindungi modalitas pembangunan dari gangguan aktor eksternal (Liebetrau & Bueger, 2024). Lemahnya tata kelola siber di negara berkembang sering kali memicu lahirnya kesenjangan kepatuhan (*compliance gap*), di mana pembangunan infrastruktur fisik siber yang masif tidak dibarengi dengan kedisiplinan regulatif, kejelasan garis komando operasional, serta penguatan kompetensi teknis sumber daya manusia yang mengelola sistem tersebut.

Kegagalan tata kelola (*governance failure*) dalam ekosistem digital dapat berujung pada kerugian sosial dan ekonomi yang sangat masif bagi kepentingan publik (Chotimah, 2019). Ketika suatu negara berkembang mempercepat migrasi layanannya ke ruang digital tanpa membangun sistem proteksi data dan manajemen risiko yang ketat, negara tersebut sedang membuka celah kerentanan yang mengundang infiltrasi aktor peretas transnasional. Serangan *ransomware* yang menyasar sektor-sektor vital pada akhirnya tidak hanya melumpuhkan operasional teknis komputer, melainkan merusak kepercayaan masyarakat terhadap stabilitas tata kelola pemerintahan (Socquet-Clerc et al., 2023). Maka dari itu, filosofi tata kelola siber yang inklusif harus menempatkan perlindungan data publik warga negara sebagai prioritas esensial yang tidak boleh dikorbankan demi percepatan pembangunan fisik semata.

Peneliti dapat merumuskan alur berpikir bahwa *cybersecurity governance* di Indonesia sepanjang periode 2020–2024 masih menyisakan celah struktural yang krusial. Ketika dikaitkan dengan pemikiran (Krahmann, 2003) mengenai desentralisasi aktor keamanan, Indonesia sebenarnya telah mencoba merangkul model multipihak

dengan melibatkan berbagai kementerian, lembaga, dan penyedia jasa teknologi untuk mengelola data publik secara bersama-sama. Namun, pergeseran dari kontrol tunggal menuju tata kelola kolektif ini tidak dibarengi dengan kejelasan batas kewenangan dan pembagian tanggung jawab hukum yang tegas jika terjadi kebocoran data. Akibatnya, ekosistem tata kelola siber di Indonesia cenderung bersifat fragmentatif dan rawan mengalami kegagalan koordinasi saat menghadapi krisis.

Kondisi fragmentasi tata kelola ini terlihat jelas dalam pola interaksi antar-lembaga pemerintah saat merespons ancaman siber transnasional. Sebagaimana ditekankan oleh (Chotimah, 2019), kehadiran BSSN seharusnya mampu bertindak sebagai lembaga komando tunggal yang mengoordinasikan seluruh kebijakan pertahanan digital nasional. Namun, dalam realitas birokrasi, tumpang tindih regulasi dan benturan kepentingan sektoral antarinstansi sering kali mengaburkan fungsi pengawasan yang dijalankan oleh BSSN. Lemahnya harmonisasi ini berujung pada lahirnya ketidakpastian hukum dan kelambatan operasional, di mana setiap instansi cenderung bergerak secara parsial tanpa kepatuhan yang seragam terhadap standar manajemen risiko siber nasional.

Jika dianalisis secara mendalam, eskalasi serangan *ransomware* transnasional yang terjadi di Indonesia selama periode 2020–2024 secara empiris berhasil mengeksploitasi kelemahan tata kelola tersebut. Ketidakpastian mengenai lembaga mana yang memiliki otoritas penuh untuk menjatuhkan sanksi yuridis terhadap kelalaian pengamanan data publik di sektor pemerintahan membuat tingkat kedisiplinan birokrasi dalam mematuhi aturan siber menjadi sangat rendah. Hambatan regulatif ini menciptakan iklim tata kelola yang reaksioner, di mana perbaikan dan evaluasi terhadap kerentanan sistem informasi vital baru dilakukan secara tergesa-gesa setelah sistem tersebut mengalami kelumpuhan total akibat serangan siber dan menjadi konsumsi publik di media massa.

Masalah tata kelola keamanan siber nasional di Indonesia juga diperparah dengan rendahnya kesadaran kolektif mengenai pentingnya akreditasi sistem

keamanan informasi dan penyediaan infrastruktur cadangan data yang memadai. Ketimpangan alokasi anggaran yang condong pada pembangunan fisik proyek digital tanpa diimbangi dengan investasi proteksi siber adalah bentuk nyata dari kegagalan perencanaan tata kelola (Krahmann, 2003). Biaya operasional untuk pengamanan siber secara berkala, audit forensik digital, serta peningkatan kapasitas keterampilan aparatur negara sering kali dipangkas demi efisiensi jangka pendek. Dampaknya, ketika sindikat peretas meluncurkan enkripsi *ransomware*, infrastruktur siber nasional tidak memiliki daya tahan sistemik untuk memulihkan layanan publik secara mandiri dalam waktu cepat.

Berdasarkan ulasan konseptual tersebut, penelitian ini memformulasikan bahwa keberhasilan penanggulangan ancaman *ransomware* transnasional di Indonesia tidak dapat dicapai hanya dengan mengandalkan pemutakhiran perangkat teknologi semata. Kerangka pemikiran (Krahmann, 2003) dan (Webber et al., 2004) memberikan landasan teoretis yang kuat bahwa perbaikan harus menyasar pada restrukturisasi pola hubungan kekuasaan, aturan kepatuhan, dan komitmen kelembagaan negara. Indonesia memerlukan transformasi tata kelola siber yang mampu menyatukan gerak birokrasi secara horizontal, mempertegas garis komando saat krisis siber terjadi, serta menegakkan akuntabilitas hukum tanpa pandang bulu terhadap setiap penyelenggara sistem elektronik yang lalai dalam menjaga keamanan data publik.

Guna mempermudah operasionalisasi Konsep *Cybersecurity Governance* ini dalam membedah kasus serangan *ransomware LockBit* 3.0 pada Bank Syariah Indonesia (2023) dan *Brain Cipher* pada Pusat Data Nasional Sementara 2 (2024), konsep ini diturunkan ke dalam dua dimensi analisis utama yang diadaptasi dari pemikiran para ahli di atas. Dimensi pertama adalah Dimensi Regulatif (*Regulatory Dimension*) yang digunakan oleh peneliti untuk mengevaluasi implementasi produk hukum formal nasional seperti regulasi pelindungan data pribadi dan aturan siber terkait dalam memaksa para penyelenggara sistem elektronik mematuhi aturan manajemen risiko dan menyediakan sistem cadangan data berlapis. Dimensi ini

menganalisis ada atau tidaknya sanksi hukum yang tegas sebagai instrumen pemaksa tata laksana siber yang disiplin di lingkungan institusi negara.

Dimensi kedua dalam operasionalisasi konsep penelitian ini adalah Dimensi Institusional (*Institutional Dimension*) yang secara khusus digunakan untuk memetakan arsitektur kelembagaan resmi, pembagian mandat darurat, serta kekokohan hubungan koordinasi horizontal lintas instansi pemerintah di bawah koordinasi lembaga siber nasional. Melalui Dimensi Institusional ini, peneliti mengevaluasi sejauh mana unit taktis operasional lapangan seperti *Computer Security Incident Response Team* (CSIRT) di berbagai sektor kritis telah siap dan terintegrasi secara fungsional untuk mengisolasi sebaran *ransomware*. Dimensi ini juga membongkar keberadaan ego sektoral antarlembaga yang sering kali menghambat jalannya mitigasi insiden dan mengorbankan keamanan data publik warga negara saat terjadi krisis siber transnasional.

Melalui penjalinan konseptual yang utuh ini, peneliti tidak sekadar menempatkan Teori Strategi Keamanan Siber Nasional dan Konsep Tata Kelola Keamanan Siber sebagai formalitas pelengkap. Kedua instrumen analitis ini justru menjadi pisau bedah yang saling mengisi untuk mengurai anatomi krisis digital di Indonesia secara lebih terarah. Ketika kerangka kerja strategis digunakan sebagai jangkar untuk mengevaluasi parameter kebijakan konkret yang diambil pemerintah, maka konsep tata kelola keamanan siber diletakkan sebagai alat untuk membongkar akar masalah struktural di lapangan, mulai dari tumpang tindih regulasi domestik hingga benturan ego sektoral antarinstansi. Pada akhirnya, dialektika antara komitmen strategi nasional dan realitas tata laksana kelembagaan inilah yang menjadi basis argumentasi utama bagi peneliti untuk mendedah respons Pemerintah Indonesia terhadap eskalasi ancaman *ransomware* transnasional periode 2020–2024 ke dalam sebuah kajian Hubungan Internasional yang utuh.

2.1.2 Teori Strategi Keamanan Siber Nasional (*National Cyber Security Strategy)*

Perkembangan ruang siber di era kontemporer telah membawa transformasi yang sangat radikal dalam lanskap keamanan global, di mana ancaman tidak lagi dapat dipahami secara konvensional melalui pendekatan kedaulatan teritorial fisik semata. Kehadiran aktor-aktor non-negara (*non-state actors*) yang memanfaatkan kecanggihan teknologi digital telah menciptakan bentuk ancaman baru yang bersifat asimetris, terdistribusi, dan lintas batas negara (*transnational*). Salah satu manifestasi ancaman yang paling destruktif bagi stabilitas ekonomi dan kedaulatan digital suatu negara adalah eskalasi serangan *ransomware* skala besar yang melumpuhkan berbagai sektor kehidupan. Fenomena transnasional ini pada akhirnya menuntut adanya pergeseran paradigma pertahanan negara dari yang semula bertumpu pada doktrin militeristik tradisional menjadi pendekatan tata kelola keamanan siber nasional yang komprehensif, inklusif, dan adaptif (Islami, 2018). Negara tidak lagi memiliki kemewahan untuk bersikap pasif, melainkan dipaksa untuk merumuskan kebijakan pertahanan non-kinetik yang terstruktur demi menjaga resiliensi nasional di ruang siber.

Dalam upaya memformulasikan respons kebijakan yang terpadu tersebut, sebuah negara membutuhkan instrumen pemandu utama yang dikenal sebagai Strategi Keamanan Siber Nasional (*National Cybersecurity Strategy*). Strategi ini bukan sekadar sebuah dokumen formal di atas kertas, melainkan sebuah doktrin dan kerangka kerja makro yang mengartikulasikan visi, misi, sasaran strategis, serta pembagian peran lintas sektoral dalam menghadapi berbagai bentuk kerentanan di ruang siber (ITU & World Bank, 2025). Melalui panduan resmi yang diterbitkan oleh *International Telecommunication Union*, sebuah strategi siber nasional yang efektif wajib menyediakan peta jalan (*roadmap*) yang holistik untuk menyinkronkan tindakan pencegahan (*prevention*), mitigasi risiko (*risk mitigation*), penanggulangan krisis (*incident response*), hingga pemulihan pasca-insiden (*disaster recovery*) (ITU, 2011). Kerangka kerja ini dirancang sedemikian rupa untuk memastikan bahwa otoritas

pemerintah, sektor swasta, akademisi, hingga masyarakat sipil bergerak dalam satu komando yang selaras untuk mengamankan aset informasi nasional dari eksploitasi peretas global (ITU, 2011).

Signifikansi dari keberadaan strategi keamanan siber nasional yang matang dan teruji secara empiris juga ditegaskan dalam kajian teoretis oleh Craig, Johnson, dan Gallop (2023). Mereka mengargumenkan bahwa tingkat kematangan dan pengembangan kapasitas siber (*cybersecurity capacity*) suatu negara tidak dapat diukur secara parsial dari kepemilikan teknologi pengamanan yang canggih semata, melainkan dari sejauh mana strategi tersebut diartikulasikan, disosialisasikan, dan diimplementasikan secara konsisten oleh institusi negara melalui kebijakan domestik maupun kolaborasi internasional. Kapasitas keamanan siber nasional merupakan hasil integrasi dinamis antara regulasi hukum yang mengikat, kesiapan kapabilitas teknis, kekokohan arsitektur kelembagaan, serta ketersediaan sumber daya manusia yang kompeten (Craig et al., 2022). Maka dari itu, analisis akademis dalam studi Hubungan Internasional terhadap efektivitas respons suatu negara dalam menghadapi infiltrasi ransomware transnasional harus didekonstruksi melalui instrumen pengukuran strategi global yang diakui secara universal (Craig et al., 2022).

Merujuk pada standardisasi internasional yang dikembangkan oleh *International Telecommunication Union* serta pemutakhiran panduan strategi siber global bersama Bank Dunia, kapasitas *National Cybersecurity Strategy* suatu negara diukur secara objektif melalui pilar tindakan fundamental (ITU & World Bank, 2025). Pilar pertama yang menjadi fondasi utama adalah Tindakan Hukum (*Legal Measures*) yang berfokus pada kodifikasi aturan hukum tertulis, perumusan undang-undang nasional, serta penyusunan regulasi turunan yang memiliki kekuatan yuridis mengikat untuk mengatur tata hidup aktor di ruang digital (ITU, 2011). Keberadaan instrumen hukum yang kuat dan responsif sangat krusial dalam menyediakan kepastian batas-batas legalitas operasional siber, menetapkan aturan kepatuhan (*regulatory compliance*) yang ketat bagi lembaga pengelola data publik, serta memberikan

landasan penegakan hukum berupa sanksi pidana maupun denda yang tegas terhadap setiap bentuk kelalaian tata laksana manajemen risiko sistem (ITU, 2011).

Pilar kedua dalam kerangka kerja strategi siber nasional adalah Tindakan Teknis (*Technical Measures*) yang menitikberatkan pada ketersediaan prosedur teknis, standarisasi sertifikasi keamanan, mekanisme pertahanan perimeter jaringan, serta pemutakhiran infrastruktur pengamanan informasi di tingkat nasional (ITU, 2011). Tindakan teknis ini mencakup pembentukan protokol deteksi dini terhadap anomali lalu lintas data, manajemen kerentanan sistem (*vulnerability management*) yang dilakukan secara berkala, hingga implementasi teknologi enkripsi mutakhir guna membentengi piringan data dari serangan siber spesifik (ITU, 2011). Tanpa adanya kesiapan teknis yang mumpuni, dinamis, dan berlapis, seluruh upaya mitigasi yang dirancang oleh negara akan sangat mudah dieksploitasi oleh aktor eksternal yang menggunakan model *Ransomware-as-a-Service* (RaaS) yang memiliki daya rusak tinggi terhadap sistem informasi (ITU & World Bank, 2025).

Pilar ketiga yang memiliki kedudukan sangat strategis dalam birokrasi pertahanan digital adalah Tindakan Organisasional (*Organizational Measures*) yang menyoroti bagaimana negara membangun arsitektur kelembagaan resmi, mendistribusikan mandat otoritas, serta merancang mekanisme komando koordinasi penanggulangan manajemen krisis siber nasional (ITU, 2011). Efektivitas pilar organisasional ini ditandai dengan hadirnya suatu lembaga pusat tunggal yang memegang mandat penuh atas strategi siber nasional seperti badan siber nasional tersentralisasi yang mampu mengikis ego sektoral dan menciptakan pola hubungan kerja sama horizontal-koordinatif antarinstansi pemerintah (ITU, 2011). Lebih jauh lagi, kesiapan pilar organisasional ini juga diukur dari pembentukan dan pengaktifan unit taktis operasional lapangan yang siap sedia merespons insiden secara cepat di berbagai sektor kritikal, atau yang dikenal sebagai *Computer Security Incident Response Team* (CSIRT) (Islami, 2018).

Pilar keempat yang menjadi penentu keberlanjutan dari keamanan siber sebuah negara adalah Peningkatan Kapasitas (*Capacity Building*) yang mencakup spektrum yang luas, mulai dari penyelenggaraan program pendidikan formal, pelatihan teknis berkelanjutan bagi aparatur sipil negara, sertifikasi kompetensi keahlian siber, hingga kampanye peningkatan kesadaran keamanan siber (*cybersecurity awareness*) secara masif di tingkat publik (ITU, 2011). Mengingat lanskap ancaman siber bergerak sangat dinamis, negara dituntut untuk memiliki pasokan talenta digital, analis forensik, dan pakar keamanan informasi yang memiliki kompetensi mendalam untuk melakukan audit kepatuhan sistem serta melacak celah keamanan. Lemahnya komitmen negara dalam melakukan investasi jangka panjang pada pilar peningkatan kapasitas SDM siber ini kerap kali menjadi faktor utama lahirnya celah kelalaian tata laksana (*human error*) fatal yang dapat meruntuhkan seluruh sistem pertahanan teknis yang telah dibangun dengan biaya mahal (Islami, 2018).

Pilar kelima dan menjadi puncak dari strategi keamanan siber nasional dalam dimensi Hubungan Internasional adalah Kerja Sama (*Cooperation*) yang menyadari bahwa arsitektur ruang siber bersifat lintas batas dan melampaui yurisdiksi teritorial konvensional, sehingga memerlukan instrumen kemitraan domestik maupun internasional (ITU, 2011). Kolaborasi internasional ini diwujudkan melalui partisipasi aktif dalam forum siber global, pertukaran intelijen ancaman (*threat intelligence sharing*), serta penyusunan mekanisme bantuan hukum timbal balik (*Mutual Legal Assistance Treaties*) guna mempermudah proses penanganan kejahatan siber transnasional (ITU & World Bank, 2025). Sinergi global ini memungkinkan suatu negara untuk membangun kesadaran situasi bersama (*global situational awareness*) dan menutup ruang gerak sindikat ransomware transnasional yang kerap berlindung di balik celah perbedaan hukum antarnegara (ITU, 2011).

Ketika mengontekstualisasikan kelima pilar strategi siber nasional tersebut ke dalam studi kasus respons Pemerintah Indonesia pada periode 2020–2024, ditemukan fakta bahwa upaya memitigasi eskalasi ransomware menghadapi tantangan struktural yang sangat kompleks di lapangan. Sebagaimana dikaji secara komprehensif oleh

Islami (2017) mengenai implementasi strategi siber Indonesia berdasarkan penilaian internasional, komitmen nasional sering kali mengalami hambatan serius akibat adanya fragmentasi birokrasi serta belum meratanya pemahaman mengenai urgensi tata kelola risiko siber di tingkat instansi publik. Meskipun pemerintah telah meluncurkan berbagai kebijakan strategis seperti Peraturan Presiden terkait keamanan siber, potret dari kerangka penilaian global secara konsisten masih menunjukkan adanya kesenjangan (*compliance gap*) yang lebar antara perumusan aturan di atas kertas dengan realisasi penegakan operasional teknis di instansi pemerintah (Islami, 2018).

Jika dibedah pada pilar hukum (*Legal Measures*), Indonesia sebenarnya telah mencatatkan pencapaian regulatif yang sangat penting melalui pengesahan Undang-Undang Pelindungan Data Pribadi (UU PDP). Secara normatif-yuridis, regulasi ini telah meletakkan standar baru yang mewajibkan seluruh penyelenggara sistem elektronik untuk menjamin keamanan, kerahasiaan, dan integritas data warga negara yang mereka kelola dari ancaman siber (Islami, 2018). Namun, fakta empiris selama rentang tahun 2020-2024 menunjukkan bahwa pilar hukum ini belum dapat ditegakkan secara maksimal karena belum meratanya integrasi aturan kepatuhan (*regulatory compliance*) di lembaga pemerintah, serta lemahnya ketegasan sanksi bagi institusi publik yang mengalami kebocoran data akibat kelalaian manajemen risiko, yang mencerminkan adanya ketidaksesuaian implementasi dari kerangka panduan siber nasional yang komprehensif (ITU & World Bank, 2025).

Kerentanan struktural yang jauh lebih mengkhawatirkan terlihat secara transparan ketika mengevaluasi pilar organisasional (*Organizational Measures*) melalui analisis studi kasus serangan ransomware pada institusi perbankan dan infrastruktur data nasional nasional periode 2020-2024. Laporan insiden menyingkap adanya masalah fragmentasi otoritas yang akut serta tumpang tindih pembagian tugas koordinasi horizontal antarinstansi pemerintah, seperti antara otoritas siber nasional selaku pengawas keamanan, kementerian teknis selaku pemilik proyek infrastruktur, dan pihak vendor pengelola operasional. Lemahnya pola hubungan koordinasi koordinatif ini menyebabkan terjadinya kelambatan penanganan darurat (*incident*

handling) saat krisis serangan ransomware terjadi, yang pada akhirnya melumpuhkan sistem layanan publik strategis dan membuktikan belum optimalnya penataan arsitektur kelembagaan resmi (ITU, 2011).

Lebih lanjut, insiden kelumpuhan total pada infrastruktur siber publik juga merefleksikan potret kelemahan pada pilar tindakan teknis (*Technical Measures*) dan peningkatan kapasitas (*Capacity Building*) di Indonesia. Berdasarkan data evaluasi pasca-insiden, terungkap fakta bahwa infeksi ransomware transnasional sering kali dipicu oleh kelalaian teknis yang sangat elemental, yakni adanya tindakan penonaktifan fitur keamanan bawaan sistem oleh operator internal serta minimnya kepatuhan terhadap standarisasi manajemen kerentanan (Islami, 2018). Fakta empiris ini diperparah dengan data bahwa sebagian besar instansi pemerintah tidak mengaktifkan sistem cadangan data (*backup*) yang aman dan terisolasi di pusat data sekunder, yang membuktikan rendahnya tingkat kepatuhan institusi terhadap prosedur manajemen risiko siber serta timpangnya alokasi anggaran operasional pengamanan jika dibandingkan dengan besarnya anggaran pengadaan infrastruktur fisik siber (Craig et al., 2022).

Berdasarkan potret empiris tersebut, landasan teoretis yang diajukan oleh Craig, Johnson, dan Gallop (2023) memberikan jika bahwa evaluasi terhadap strategi keamanan siber nasional Indonesia harus diarahkan pada reformasi kapabilitas yang berorientasi jangka panjang dan adaptif. Pemerintah Indonesia tidak boleh terus-menerus terjebak pada pola respons pertahanan yang bersifat reaksioner dan tambal sulam, di mana perbaikan sistem baru dilakukan secara tergesa-gesa setelah terjadi insiden kebocoran data publik yang masif. Strategi siber harus dikonstruksikan dengan indikator pencapaian kinerja yang terukur (*Key Performance Indicators*), diintegrasikan secara penuh ke dalam prioritas kebijakan nasional, serta didukung dengan komitmen tata kelola anggaran yang proporsional demi menjaga kedaulatan digital negara dari ancaman asimetris (ITU & World Bank, 2025).

Akibatnya upaya penguatan kedaulatan digital dan resiliensi nasional Indonesia dalam menghadapi ancaman transnasional ransomware di masa depan sangat bergantung pada konsistensi penegakan kelima pilar *National Cybersecurity Strategy* secara simultan dan terintegrasi. Otoritas eksekutif wajib memastikan bahwa regulasi hukum tidak hanya tajam ke sektor swasta melainkan harus ditegakkan secara tegas dan adil di lingkungan instansi publik pengelola data (Islami, 2018). Penerapan sanksi administratif, audit kepatuhan siber berkala, dan kejelasan tanggung jawab hukum bagi penyelenggara sistem elektronik harus dijalankan secara konsekuen guna memaksa birokrasi pemerintahan meningkatkan disiplin tata laksana data publik mereka sesuai prinsip akreditasi sistem informasi internasional (ITU & World Bank, 2025).

Pada dimensi institusional dan organisasional, langkah taktis yang harus segera direalisasikan adalah memperkuat posisi lembaga siber terpusat sebagai institusi komando tunggal dalam manajemen krisis siber nasional, guna menghapus tembok ego sektoral antarlembaga pemerintah yang selama ini menghambat koordinasi. Percepatan pembentukan dan standardisasi kapasitas tim taktis CSIRT di seluruh kementerian, lembaga, dan daerah tidak boleh hanya berhenti pada tataran kuantitas kuota pembentukan semata, melainkan wajib diimbangi dengan pelatihan peningkatan kapasitas SDM secara berkala (Islami, 2018). Kedisiplinan para operator teknologi informasi dalam mematuhi standar operasional prosedur (SOP) keamanan sistem mutlak diperketat agar kelalaian teknis elementer tidak kembali menjadi celah masuknya aktor kejahatan siber internasional (Craig et al., 2022).

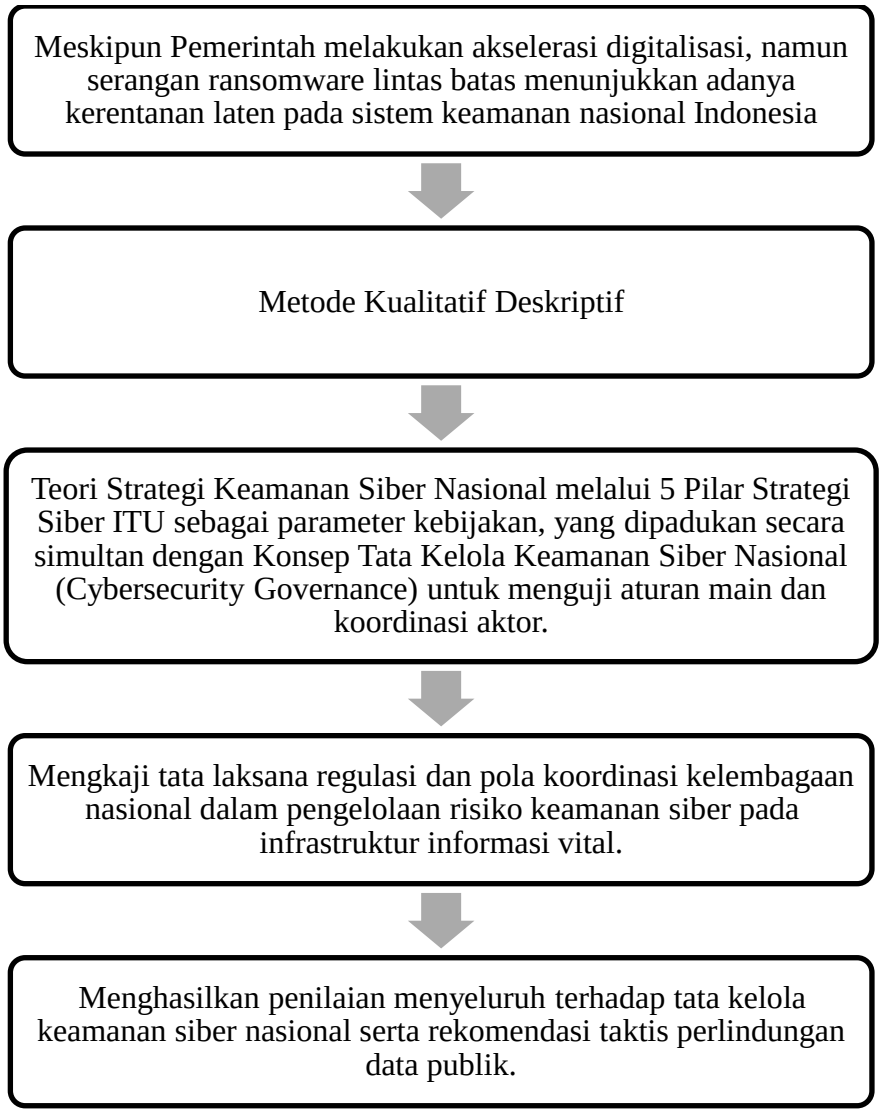
Sebagai sintesis akhir, keberhasilan strategi pertahanan siber Indonesia dalam merespons ancaman ransomware transnasional periode 2020–2024 pada akhirnya ditentukan oleh komitmen politik negara untuk mengeksekusi lima pilar strategi ITU secara konsisten. Melalui sinkronisasi tindakan hukum yang tegas, pemutakhiran standar tindakan teknis yang mutakhir, konsolidasi kelembagaan organisasional yang solid, perluasan investasi peningkatan kapasitas SDM, serta penguatan jaringan kerja sama intelijen siber internasional, Indonesia akan mampu mengikis *compliance gap* yang selama ini terjadi (ITU & World Bank, 2025). Transformasi strategi ini akan

menjadi pilar penyangga utama yang mengamankan infrastruktur informasi vital nasional, melindungi hak privasi data publik warga negara, sekaligus menegakkan kedaulatan siber Indonesia di tengah dinamika anarki ruang digital global (Craig et al., 2022).

2.2. Kerangka Pemikiran

Dalam penelitian ini, kerangka pemikiran digunakan sebagai instrumen konseptual untuk membangun pola pikir yang terstruktur sekaligus memvisualisasikan postur ketangguhan operasional yang diupayakan oleh Pemerintah Indonesia dalam merespons ancaman siber lintas batas. Strategi negara dalam memproteksi keamanan data nasional dikaji secara spesifik melalui Konsep Tata Kelola Keamanan Siber Nasional guna memetakan pola koordinasi horizontal antar-aktor strategis, sinkronisasi regulasi, serta implementasi struktur organisasi dalam menjaga stabilitas sistem informasi. Konstruksi analisis ini kemudian dipertajam menggunakan Teori Strategi Keamanan Siber Nasional yang dijabarkan melalui 5 Pilar Strategi Keamanan Siber ITU mencakup aspek legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional sebagai pisau analisis utama untuk mengevaluasi resiliensi Infrastruktur Informasi Vital (IIV) dari serangan *ransomware* transnasional periode 2020–2024. Melalui kerangka ini, peneliti menyajikan alur pemikiran yang menghubungkan seluruh variabel penelitian guna menjawab rumusan masalah secara sistematis dengan mempertimbangkan kompleksitas tata kelola dan tantangan implementasi pada setiap pilar strategi siber.

Gambar 2. 1 Kerangka Pemikiran Penelitian



Sumber: diolah oleh peneliti untuk keperluan penelitian

III. METODOLOGI PENELITIAN

Pada bab ini peneliti akan menjelaskan metodologi penelitian yang digunakan dan bertujuan untuk memberikan gambaran mengenai kerangka kerja serta langkah-langkah sistematis yang diambil untuk mengkaji fenomena yang diteliti. Bab ini terbagi ke dalam lima bagian utama, yaitu: jenis penelitian, fokus penelitian, sumber data, teknik pengumpulan data, serta teknik analisis data. Dalam penelitian ini, peneliti menggunakan pendekatan kualitatif deskriptif dengan fokus penelitian yaitu pada analisis strategi keamanan siber yang diimplementasikan oleh Indonesia terhadap serangan ransomware pada sektor layanan publik dan perbankan pada rentang waktu 2020-2024. Untuk menjawab rumusan masalah, peneliti menggunakan sumber-sumber data sekunder yang dikumpulkan melalui teknik studi literatur. Data dan fakta yang telah terkumpul kemudian akan dianalisis menggunakan teknik reduksi data dan divalidasi melalui strategi triangulasi sumber untuk menjamin kredibilitas temuan.

3.1. Jenis Penelitian

Dalam penelitian ini, peneliti menerapkan pendekatan kualitatif. Sebagaimana dijelaskan oleh (Bryman, 2016), penelitian kualitatif dapat dipahami sebagai strategi penelitian yang umumnya menekankan penggunaan kata-kata daripada kuantifikasi dalam proses pengumpulan dan analisis data. Pendekatan ini bersifat induktif, interpretatif, serta konstruktif secara sosial. Melalui studi ini, peneliti bertujuan untuk mengeksplorasi berbagai fenomena secara mendalam dan kronologis.

Penelitian ini secara khusus dirumuskan sebagai studi kasus. Merujuk pada definisi (Creswell, 2009), studi kasus adalah strategi penelitian untuk eksplorasi

mendalam atas sebuah kasus yang terbatasi *(bounded*). Dalam konteks ini, strategi keamanan siber Indonesia (diposisikan sebagai program dan proses) dalam menghadapi serangan ransomware (diposisikan sebagai peristiwa dan aktivitas) ditetapkan sebagai kasus yang diteliti. Batasan penelitian ini mengikuti kerangka Creswell (2009) yang mencakup batasan temporal, yaitu periode 2020-2024, dan batasan aktivitas. Strategi ini dianggap relevan untuk mengungkap wawasan yang komprehensif dan mendalam atas fenomena tersebut.

Dengan mengacu pada topik penelitian ini, adapun langkah-langkah utama yang digunakan peneliti dalam penelitian ini ialah (1) memunculkan permasalahan riset secara umum terkait bagaimana strategi keamanan siber Indonesia dalam menangani serangan ransomware dilaksanakan; (2) seleksi subjek yang relevan berkaitan dengan strategi keamanan siber Indonesia, seperti Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika; (3) pengumpulan data yang dianggap relevan dari sumber-sumber sekunder yang kredibel seperti dokumen kebijakan, laporan teknis BSSN, dan jurnal-jurnal terkait; (4) interpretasi data terkait strategi keamanan yang coba dibangun oleh Indonesia; (5) membangun kerangka konseptual berdasarkan interpretasi data; (5) memfokuskan pertanyaan penelitian dan pengumpulan data tambahan; dan (6) menuliskan temuan serta konklusi terkait strategi keamanan siber Indonesia tersebut. Keseluruhan proses yang terdiri dari enam langkah tersebut diharapkan mampu mengarahkan peneliti untuk menjawab pertanyaan penelitian secara komprehensif.

3.2. Fokus Penelitian

Fokus dalam penelitian ini ialah melihat bagaimana strategi keamanan siber Indonesia dalam menangani serangan *ransomware*. Dalam rentang waktu yang cukup panjang, peneliti memfokuskan penelitian ini pada upaya keamanan siber yang dibangun pada tahun 2020 sampai dengan 2024. Alasan pemilihan rentang waktu tersebut adalah

karena periode ini menandai eskalasi dramatis serangan siber terhadap infrastruktur kritikal Indonesia. Dalam penelitian ini, peneliti akan memfokuskan riset ini hanya kepada upaya dan strategi keamanan siber yang dilakukan oleh Indonesia, dan bukan sebaliknya (menganalisis strategi pelaku serangan). Alasannya ialah karena Lebih spesifik, fokus penelitian ini akan menganalisis kebijakan keamanan siber pada kasus peretasan Pusat Data Nasional (PDN) dan Bank Syariah Indonesia (BSI). Analisis kualitatif ini dikaji melalui indikator dari Teori Strategi Keamanan Siber Nasional yang dijabarkan ke dalam 5 Pilar Strategi Keamanan Siber ITU yakni pilar legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional guna menilai sejauh mana Pemerintah Indonesia mampu menjaga resiliensi Infrastruktur Informasi Vital (IIV) dari ancaman *ransomware*. Selain itu, kajian ini juga dipertajam menggunakan Konsep Tata Kelola Keamanan Siber Nasional untuk memetakan bagaimana tata laksana regulasi serta pola koordinasi horizontal antar-aktor strategis, seperti BSSN, Kominfo, dan operator sektor kritis, dijalankan dalam merespons ancaman siber transnasional.

3.3. Sumber Data

Penelitian ini menggunakan sumber-sumber data sekunder. Sesuai dengan kategorisasi oleh Alan Bryman (2016), peneliti mengumpulkan data yang bersumber dari dokumen resmi terkait, seperti dokumen kebijakan, cetak biru strategi, serta laporan tahunan yang dipublikasikan oleh Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika (Kemenkominfo). Peneliti juga menggunakan laporan analisis ancaman dari lembaga riset keamanan siber independen dan mitra internasional, misalnya laporan dari CISA atau World Economic Forum (WEF), yang mana oleh John W. Creswell (2009) dikategorikan sebagai dokumen publik . Selain itu, data juga bersumber dari literatur akademik seperti artikel-artikel yang dipublikasikan dalam jurnal ilmiah, buku, serta penelitian terdahulu yang relevan . Terakhir, peneliti memanfaatkan arsip berita dari media massa yang kredibel untuk

merekonstruksi dan mendokumentasikan studi kasus spesifik , sebagai contoh insiden yang menimpa Bank Syariah Indonesia (BSI) dan Pusat Data Nasional (PDN).

3.4. Teknik Pengumpulan Data

Dalam mengumpulkan data, peneliti menggunakan teknik studi literatur dengan mempelajari dokumen. (Creswell, 2009) menjelaskan bahwa studi literatur memiliki beberapa tujuan, di antaranya adalah untuk membagikan hasil studi lain yang terkait erat dengan penelitian yang sedang dilakukan, dan untuk menghubungkan penelitian dengan dialog yang lebih besar yang sedang berlangsung dalam literatur . Adapun data yang dikumpulkan berupa dokumen dan laporan yang menjabarkan strategi keamanan siber yang diimplementasikan oleh Indonesia, rincian insiden serangan ransomware besar (seperti serangan terhadap BSI dan PDNS), laporan teknis dari BSSN mengenai deteksi dan respons insiden, serta data pendukung lainnya yang relevan untuk menganalisis efektivitas strategi tersebut selama periode 2020-2024 . Peneliti terus memastikan bahwa data yang dikumpulkan berasal dari sumber-sumber terpercaya dan terbaru agar hasil penelitian ini dapat disajikan dengan sebaik-baiknya dan mampu membawa manfaat bagi semua kalangan.

3.5. Teknik Analisis Data

Dalam menganalisis data yang telah dikumpulkan, peneliti menggunakan kerangka kerja analisis data kualitatif yang dikemukakan oleh Matthew B. Miles, A. Michael Huberman, dan Johnny Saldaña (2014). (Miles et al., 2014) menjelaskan bahwa analisis data kualitatif terdiri dari tiga alur kegiatan yang terjadi secara bersamaan (*concurrent flows of activity*), yaitu: kondensasi data (*data condensation*), penyajian data (*data display*), dan penarikan/verifikasi kesimpulan (*conclusion drawing/verification*) .

Tahap pertama adalah kondensasi data, yang didefinisikan sebagai proses memilih, memfokuskan, menyederhanakan, mengabstraksi, dan/atau mentransformasi data yang terdapat dalam catatan lapangan, transkrip, dokumen, dan materi empiris lainnya (Miles et al. 2014). Pada tahap ini, peneliti mereduksi data yang diperoleh dari berbagai laporan resmi, dokumen kebijakan, dan sumber daring lainnya untuk memilih serta mengerucutkan data agar lebih terfokus dan spesifik dalam mendukung proses analisis data.

Tahap kedua adalah penyajian data. (Miles et al., 2014) mendefinisikan penyajian data sebagai kumpulan informasi yang terorganisir dan padat yang memungkinkan penarikan kesimpulan. Pada tahap ini, peneliti akan menyajikan data historis dan dokumen kebijakan yang telah direduksi untuk kemudian dianalisis secara kritis menggunakan pisau analisis Teori Strategi Keamanan Siber Nasional yang dioperasionalisasikan melalui 5 Pilar Strategi Keamanan Siber ITU yakni pilar legal, teknis, organisasi, pengembangan kapasitas, serta kerja sama internasional. Selain itu, analisis juga diarahkan pada Konsep Tata Kelola Keamanan Siber Nasional guna memetakan pola koordinasi dan tata laksana kelembagaan dalam melindungi sektor layanan publik serta perbankan dari ancaman siber transnasional.

Tahap akhir adalah penarikan dan verifikasi kesimpulan. Sejak awal pengumpulan data, peneliti kualitatif mulai menginterpretasi makna dari apa yang ia lihat, dengar, dan baca. Makna yang muncul dari data harus diuji untuk plausibilitas, keteguhan, dan konfirmabilitasnya yaitu, validitasnya (Miles et al., 2014). Pada tahap akhir ini, peneliti akan menarik kesimpulan berdasarkan data yang telah direduksi dan disajikan, yang telah dielaborasikan dengan kerangka konseptual yang digunakan.

Untuk menghindari subjektivitas dalam penelitian ini, peneliti juga melakukan teknik analisis triangulasi data . (Creswell, 2009) mendefinisikan triangulasi sebagai proses *different data sources of information by examining evidence from the sources and using it to build a coherent justification for themes* . Dalam konteks penelitian ini, peneliti menggunakan triangulasi sumber untuk menguji validitas penelitian. Data tersebut berasal dari berbagai pihak, yaitu lembaga pemerintah Indonesia (seperti

BSSN dan Kemenkominfo) , laporan dari perusahaan keamanan siber dan lembaga riset internasional , serta pihak netral, seperti laporan akademis dan artikel media internasional yang kredibel.

V. SIMPULAN DAN SARAN

Bab ini menyajikan sintesis akhir dari keseluruhan rangkaian analisis yang telah dilakukan mengenai tata laksana dan implementasi Konsep Tata Kelola Keamanan Siber Nasional serta pemenuhan pilar Teori Strategi Keamanan Siber Nasional di Indonesia dalam menghadapi eskalasi ancaman ransomware transnasional pada periode 2020–2024. Melalui penelusuran mendalam terhadap berbagai data, bab ini merangkum temuan-temuan krusial yang menjawab rumusan masalah penelitian, sekaligus merumuskan sejumlah saran strategis baik secara praktis maupun akademis guna memberikan kontribusi bagi pengembangan studi Hubungan Internasional, khususnya dalam lingkup kajian tata kelola data publik di masa mendatang.

5.1. Simpulan

Berdasarkan keseluruhan hasil penelitian dan pembahasan yang telah dipaparkan pada bab sebelumnya, peneliti menyimpulkan bahwa keamanan siber nasional Indonesia saat ini berada pada titik krusial yang menuntut perhatian serius dari seluruh pemangku kepentingan. Transformasi digital yang berlangsung sangat cepat di berbagai sektor pemerintahan dan bisnis tidak dibarengi dengan kesiapan infrastruktur serta regulasi yang memadai, sehingga menciptakan celah yang lebar bagi aktor jahat untuk melancarkan serangan siber. Keamanan siber tidak lagi hanya sekadar urusan teknis di level departemen teknologi informasi, melainkan telah menjadi isu kedaulatan negara yang menyentuh stabilitas ekonomi, kepercayaan publik, dan keberlangsungan layanan publik. Maka dari itu, diperlukan pergeseran paradigma dari pendekatan yang

reaktif menuju strategi pertahanan yang proaktif, integratif, dan berbasis pada manajemen risiko yang komprehensif.

Permasalahan mendasar yang ditemukan dalam tata kelola keamanan siber nasional adalah fragmentasi regulasi dan koordinasi kelembagaan yang masih terjebak dalam ego sektoral yang sangat kaku. Ketidaksinkronan aturan antar kementerian dan lembaga menciptakan *compliance gap* yang dimanfaatkan oleh peretas untuk melumpuhkan sistem vital, seperti yang terbukti pada kasus peretasan BSI dan PDNS 2. Regulasi yang ada saat ini masih bersifat parsial dan belum mampu menjadi payung hukum yang kuat untuk menegakkan kepatuhan di seluruh instansi pemerintah pusat maupun daerah. Reformasi regulasi harus segera dilakukan agar tercipta satu standar keamanan siber nasional yang mengikat dan memiliki daya paksa bagi seluruh penyelenggara sistem elektronik nasional.

Sinergi antarlembaga yang lemah menjadi faktor utama mengapa insiden siber berskala nasional seperti peretasan PDNS 2 bisa menyebabkan lumpuhnya sistem secara massal dan berhari-hari. Tanpa adanya koordinasi yang efektif, setiap instansi cenderung bergerak sendiri-sendiri tanpa memikirkan risiko *lateral movement* yang bisa terjadi antar jaringan yang terhubung. Komando tunggal yang memiliki otoritas penuh dalam penanganan krisis siber menjadi kebutuhan mutlak agar respon terhadap serangan tidak lagi lamban dan terpecah-pecah. Perlu dibentuk sebuah mekanisme koordinasi yang mengintegrasikan seluruh elemen pertahanan siber, mulai dari lembaga siber, sektor pertahanan, hingga sektor komunikasi, guna menjamin respon yang cepat dan terarah.

Kemandirian teknologi juga menjadi poin penting yang disimpulkan dari kerentanan infrastruktur digital yang kita miliki saat ini, terutama ketergantungan pada vendor pihak ketiga yang sering kali tidak memenuhi standar keamanan yang diinginkan. Kedaulatan digital tidak akan tercapai selama infrastruktur inti dikelola oleh entitas yang tidak sepenuhnya berada dalam pengawasan dan kendali nasional yang ketat. Investasi pada riset dan pengembangan teknologi keamanan siber dalam

negeri harus menjadi prioritas, agar Indonesia memiliki kendali penuh atas sistem dan perangkat yang melindungi data strategis negara. Kemandirian ini adalah kunci agar kebijakan keamanan siber nasional tidak mudah dipengaruhi oleh kepentingan politik atau celah keamanan yang disengaja oleh penyedia teknologi asing.

Selain aspek teknis dan regulasi, faktor sumber daya manusia menjadi mata rantai terlemah dalam ekosistem keamanan siber di Indonesia, di mana minimnya tenaga ahli yang kompeten menghambat efektivitas pertahanan nasional. Program peningkatan kompetensi ASN dan profesional siber harus dilaksanakan secara masif, terukur, dan berkelanjutan untuk menutup kesenjangan talenta digital yang semakin nyata di era Society 5.0. Pelatihan bukan hanya mengenai teknis pengamanan sistem, tetapi juga mengenai pembentukan budaya keamanan siber di mana setiap individu merasa bertanggung jawab atas setiap aset data yang mereka kelola. Tanpa investasi pada manusia, sistem pertahanan siber yang secanggih apapun akan dengan mudah ditembus oleh teknik *social engineering* yang sederhana.

Pentingnya peran kepemimpinan dalam mengarusutamakan keamanan siber ke dalam prioritas strategis organisasi tidak bisa lagi dinegosiasikan. Sering kali, keamanan siber dianggap sebagai beban biaya, padahal investasi pada keamanan adalah bentuk mitigasi terhadap potensi kerugian ekonomi dan sosial yang jauh lebih besar. Pimpinan tertinggi di instansi pemerintah dan sektor perbankan harus terlibat langsung dalam pengawasan dan penetapan kebijakan keamanan siber di lingkup tanggung jawab mereka. Kesadaran kepemimpinan akan menentukan sejauh mana budaya keamanan siber akan tumbuh dan mengakar di dalam organisasi.

Dalam konteks pelayanan publik, keamanan data masyarakat adalah bentuk nyata dari tanggung jawab negara terhadap perlindungan privasi warganya di ruang digital. Kegagalan menjaga data nasional bukan hanya kegagalan administratif, tetapi merupakan pelanggaran hak asasi yang dapat menurunkan legitimasi pemerintah. Perlindungan data nasional harus dijamin oleh sistem yang *resilient*, di mana redundansi data dan sistem pemulihan bencana (*Disaster Recovery*) menjadi komponen

wajib yang tidak bisa ditawar lagi. Setiap instansi harus memiliki jaminan bahwa data masyarakat tetap aman dan dapat diakses meskipun sistem utama sedang mengalami gangguan atau serangan.

Kerja sama internasional dalam hal pertukaran informasi mengenai ancaman siber dan penegakan hukum lintas batas harus terus ditingkatkan. Ancaman siber tidak mengenal batas wilayah negara, sehingga hanya melalui kerjasama global yang erat kita dapat memutus rantai kelompok peretas transnasional. Partisipasi aktif Indonesia dalam forum internasional, serta adopsi standar siber global yang disesuaikan dengan kebutuhan nasional, akan memperkuat posisi tawar Indonesia dalam diplomasi siber. Sinergi internasional bukan berarti kehilangan kedaulatan, melainkan memperkuat pertahanan nasional melalui dukungan komunitas global yang memiliki visi serupa.

Perlunya undang-undang khusus mengenai tindak pidana siber menjadi desakan yang semakin nyata agar aparat penegak hukum memiliki perangkat yang memadai untuk bertindak. Saat ini, penegakan hukum seringkali terhambat oleh keterbatasan bukti digital dan aturan yang belum mampu memfasilitasi investigasi siber yang cepat. Kejelasan hukum mengenai tindak pidana siber akan memberikan kepastian bagi masyarakat dan efek jera yang nyata bagi para pelaku kriminal siber. Sinergi antara penegak hukum dan lembaga keamanan siber harus diperkuat agar investigasi dapat dilakukan secara saintifik dan efektif dalam setiap insiden siber yang terjadi.

Budaya keamanan siber harus ditanamkan sejak dini melalui pendidikan formal maupun edukasi kepada masyarakat luas agar ekosistem digital kita menjadi lebih tangguh. Kerentanan yang terjadi saat ini tidak lepas dari minimnya literasi digital yang aman di tingkat pengguna akhir yang sering menjadi pintu masuk bagi serangan siber. Program kesadaran siber nasional harus menyasar seluruh lapisan masyarakat, agar setiap individu memiliki kewaspadaan yang tinggi terhadap ancaman digital. Kesadaran publik adalah lapisan pertahanan pertama yang paling efektif sebelum serangan menembus masuk ke jaringan yang lebih dalam.

Kemandirian dalam audit keamanan siber oleh lembaga independen yang profesional dan memiliki otoritas tinggi sangat penting untuk menjaga integritas sistem. Audit bukan untuk mencari kesalahan, melainkan untuk memberikan gambaran obyektif mengenai kondisi sistem dan memberikan rekomendasi perbaikan yang sifatnya mengikat. Selama ini, audit sering kali hanya dilakukan sebagai formalitas dan tidak memberikan dampak perbaikan yang berarti bagi sistem. Ke depan, hasil audit harus menjadi dasar bagi perbaikan sistem dan pemberian alokasi anggaran bagi setiap instansi pemerintah agar sistem mereka mencapai level kematangan yang memadai.

Pemanfaatan kecerdasan buatan (*Artificial Intelligence*) dalam keamanan siber harus dikelola dengan bijak sebagai alat bantu untuk deteksi dini dan pemulihan otomatis. Namun, integrasi teknologi AI harus dibarengi dengan pengawasan ketat agar tidak menimbulkan celah keamanan baru bagi sistem nasional. Sinergi antara pakar AI dan pakar siber adalah keharusan agar teknologi terbaru dapat dimanfaatkan secara aman tanpa mengorbankan keamanan data. Teknologi harus dikendalikan oleh manusia yang berpengetahuan, bukan sebaliknya.

Komunikasi publik saat terjadi krisis siber harus diatur dengan protokol yang jelas agar tidak menimbulkan kepanikan yang tidak perlu di tengah masyarakat. Kegagalan dalam memberikan informasi yang benar kepada publik saat serangan BSI dan PDNS 2 terbukti memperburuk suasana dan menurunkan kepercayaan terhadap pemerintah. Komunikasi yang transparan, jujur, dan berorientasi pada penyelesaian masalah harus menjadi protokol tetap bagi setiap instansi yang terkena serangan siber. Kepercayaan masyarakat adalah modal sosial termahal yang harus dijaga melalui komunikasi yang efektif selama krisis berlangsung.

Pentingnya menjaga *supply chain security* atau keamanan rantai pasok teknologi menjadi sorotan baru yang harus dimasukkan ke dalam kerangka pertahanan nasional kita. Mengingat sebagian besar komponen sistem kita berasal dari vendor global, maka verifikasi keamanan terhadap perangkat keras dan lunak yang digunakan adalah mutlak. Sinergi kelembagaan harus menjamin adanya mekanisme sertifikasi

keamanan yang ketat bagi setiap vendor yang ingin bekerja sama dengan instansi pemerintah. Kita harus memastikan bahwa setiap komponen yang masuk ke dalam jaringan nasional adalah komponen yang bersih dari *backdoor* atau kerentanan tersembunyi.

Pembangunan pusat data nasional harus dikelola dengan standar yang melampaui standar pusat data komersial, mengingat betapa tingginya risiko serangan terhadap infrastruktur data nasional. Sinergi antara pengelola pusat data dan otoritas siber nasional harus memastikan adanya pengawasan terus-menerus terhadap trafik dan aktivitas mencurigakan yang terjadi di dalam pusat data tersebut. Keamanan pusat data nasional bukan sekadar masalah teknis infrastruktur fisik, tetapi masalah bagaimana data tersebut diamankan secara logis di setiap lapisannya. Kedaulatan data nasional sangat bergantung pada betapa ketat dan aman pengelolaan pusat data tersebut.

Ketahanan siber nasional memerlukan kolaborasi antar sektor yang lebih luas, termasuk dengan sektor akademisi yang memiliki potensi riset keamanan siber yang sangat besar. Sinergi antara dunia akademis dan instansi pemerintah akan membantu dalam pengembangan solusi keamanan siber yang bersifat inovatif dan aplikatif di lapangan. Riset yang mendalam mengenai pola serangan dan teknologi pertahanan terbaru harus menjadi landasan bagi perumusan kebijakan siber nasional di masa depan. Kerjasama antara pemerintah, industri, dan akademisi adalah bentuk dari *triple helix* yang harus diperkuat untuk menghadapi tantangan siber yang semakin kompleks.

Membangun ketahanan siber juga harus memperhatikan aspek privasi data masyarakat sebagai hak yang harus dijamin oleh negara dalam setiap sistem yang dibangun. Privasi bukan sesuatu yang dapat dikorbankan demi efisiensi sistem, tetapi harus menjadi bagian dari desain sistem itu sendiri sejak awal dikembangkan. Negara memiliki kewajiban moral dan hukum untuk memastikan bahwa data masyarakat tidak disalahgunakan, baik oleh pihak internal maupun eksternal. Perlindungan privasi adalah pilar utama dari kepercayaan publik terhadap pemerintahan digital.

Keamanan siber di era Society 5.0 adalah tentang bagaimana kita melindungi masyarakat dari bahaya digital tanpa membatasi kebebasan mereka untuk berinovasi dan berkarya di ruang siber. Strategi keamanan siber harus bersifat memfasilitasi, bukan membatasi, sehingga setiap elemen bangsa merasa aman untuk memanfaatkan teknologi untuk kemajuan bersama. Sinergi yang dibangun harus bersifat inklusif, yang melibatkan berbagai pemangku kepentingan untuk bekerja bersama dalam menciptakan ekosistem digital yang sehat dan aman. Keamanan dan kenyamanan harus berjalan beriringan dalam setiap langkah transformasi digital yang kita tempuh.

Tantangan serangan siber di masa depan akan semakin sulit diprediksi, sehingga ketahanan siber nasional harus senantiasa ditingkatkan dan disempurnakan tanpa henti. Tidak ada sistem yang seratus persen aman, namun dengan kerja keras dan komitmen kolektif, kita dapat meminimalisir risiko hingga ke level yang dapat diterima oleh organisasi. Proses ini membutuhkan dedikasi jangka panjang dari seluruh elemen bangsa, mulai dari tingkat pimpinan tertinggi hingga masyarakat pengguna teknologi. Ketahanan siber adalah perjalanan panjang, bukan tujuan akhir yang bisa dicapai dalam waktu singkat.

Kedaulatan digital Indonesia di masa depan sangat ditentukan oleh seberapa serius kita dalam membangun sinergi kelembagaan dan ketahanan siber nasional saat ini. Kasus BSI dan PDNS 2 harus dijadikan pelajaran berharga bagi bangsa ini untuk berbenah dan mengakhiri budaya kerja yang tidak terkoordinasi. Dengan menjadikan keamanan siber sebagai prioritas nasional yang nyata, didukung oleh sinergi antarlembaga yang kokoh, SDM yang unggul, dan kepemimpinan yang berwawasan luas, Indonesia akan mampu melangkah dengan percaya diri di tengah era Society 5.0. Ketahanan siber nasional adalah harga mati demi terwujudnya bangsa yang berdaulat, mandiri, dan mampu memberikan pelayanan terbaik bagi seluruh rakyatnya di ruang siber.

5.2. Saran

Berdasarkan pada simpulan yang telah dijabarkan sebelumnya, maka peneliti merumuskan beberapa saran yang diharapkan dapat memberikan kontribusi secara praktis maupun akademis. Adapun saran-saran tersebut, antara lain:

a. Kepada para pengkaji Hubungan Internasional untuk dapat berkontribusi terhadap penggalian informasi dan paparan yang lebih mendetail serta spesifik pada langkah-langkah strategi Teori Strategi Keamanan Siber Nasional yang dilakukan oleh Pemerintah Republik Indonesia dalam meredam dampak serangan *ransomware*. Dengan demikian, temuan-temuan yang lebih mendetail serta spesifik mendorong kualitas penelitian menjadi lebih baik serta mampu membawa dampak praktis dan akademis kepada banyak pihak, khususnya akademisi dan praktisi kajian keamanan siber.

DAFTAR PUSTAKA

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699.

Adma, A., Surbakti, Y. M., & Sari. (2023). Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan. Jurnal Kajian Stratejik Ketahanan Nasional 6 (1). https://doi.org/10.7454/jkskn.v6i1.10077.

Adristi, F. I., & Ramadhani, E. (2024). Analisis dampak kebocoran data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan matriks budaya keamanan siber dan dimensi budaya nasional Hofstede. Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen, 2(6), 196–212. https://journal.uii.ac.id/selma/article/view/3552.

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analisis ancaman kejahatan siber bagi keamanan nasional pada masa pandemi COVID-19. Jurnal Kajian Stratejik Ketahanan Nasional, 4(2). https://doi.org/10.7454/jkskn.v4i2.10052.

Aggarwal, Manuj. (2023). Ransomware Attack: An Evolving Targeted Threat. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, July 6, 1–7. https://doi.org/10.1109/ICCCNT56998.2023.10308249.

Akinyemi, O., Sulaiman, R., & Abosata, N. (2023). *Analysis of the LockBit 3.0 and its infiltration into Advanced's infrastructure crippling NHS services* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2308.05565.

Annisa, S., & Langi, A. R. (2025). Evaluasi strategi reaktif pasca serangan ransomware pada Pusat Data Nasional Sementara 2 Surabaya. Prosiding Seminar Nasional Sains dan Teknologi Seri III, 2(1), 680–691.

Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & 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.

Bryman, Alan. (2016). Social Research Methods. Fifth edition. Oxford University Press.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO), 3, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. Politica: Jurnal Masalah Politik Dalam Negeri, 10(2), 113–128. https://doi.org/10.22212/jp.v10i1.1447.

Craig, Anthony J. S., Richard A. I. Johnson, and Max Gallop. (2022). Building Cybersecurity Capacity: A Framework of Analysis for National Cybersecurity Strategies. *Journal of Cyber Policy* 7 (3): 375–98. https://doi.org/10.1080/23738871.2023.2178318.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). SAGE Publications.

Darumaya, B. A., Maarif, S., Toruan, T. S. L., & Swastanto, Y. (2023). Pemikiran potensial ancaman perang siber di Indonesia: Suatu kajian strategi pertahanan. *Jurnal Keamanan Nasional*, *9*(2), 299–324. https://ejurnal.ubharajaya.ac.id/index.php/kamnas/article/view/584

Disantara, F. P. (2021). Tripartite collaborative institutions: Skema konvergensi institusi untuk mewujudkan ketahanan siber Indonesia. *Istinbath: Jurnal Hukum*, 18(2), 194–215. https://doi.org/10.32332/istinbath.v18i2.3641.

Dwiaji, L., Widodo, A. M., Firmansyah, G., & Tjahyono, B. (2024). Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector. Asian Journal of Social and Humanities 2 (6): 1341–53. https://doi.org/10.59888/ajosh.v2i6.261.

Dyahtaryani, L. R., & Trianto, N. (2024). Analysis of defense and cyber security in airspace management in Indonesia. *Lex Laguens: Jurnal Kajian Hukum*, *2*(1). https://jurnal.dokterlaw.com/index.php/lexlaguens/article/view/57.

Fazri, Raden Mochammad. (2026). *Adoption of Cyber Security Maturity Framework for Data Protection in Higher Education*.

Ginanjar, Yusep. (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.

Hansel, M., & Silomon, J. (2024). Ransomware as a threat to peace and security: Understanding and avoiding political worst-case scenarios. Journal of Cyber Policy, 9(2), 159–178. https://doi.org/10.1080/23738871.2024.2357092.

Hapizon, M. R., Rizki, K., & Mahmuluddin. (2023). Analisis kerjasama cyber security Indonesia-Australia dalam menangani kejahatan siber di Indonesia. Universitas Mataram.

Ikhssani, A., Mudra, C., & Prasidya, F. G. (2024). Cybersecurity dan tata kelola intelijen. Jurnal Kajian Stratejik Ketahanan Nasional, 7(1). https://doi.org/10.7454/jkskn.v7i1.10086.

International Telecommunication Union. (2021). *Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity*. ITU. https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2021.

International Telecommunication Union, Commonwealth Secretariat, Geneva Centre for Security Sector Governance, Global Cyber Security Capacity Centre, Cyber Security Agency of Singapore, & The World Bank. (2025). *Guide to developing a national cybersecurity strategy* (2nd ed.). ITU. https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2025.

Islami, M. J. (2018). Tantangan dalam implementasi strategi keamanan siber nasional Indonesia ditinjau dari penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi, 8*(2), 137. https://doi.org/10.17933/mti.v8i2.108.

Khoironi, S. C. (2020). Pengaruh analisis kebutuhan pelatihan budaya keamanan siber sebagai upaya pengembangan kompetensi bagi Aparatur Sipil Negara di era

digital. Jurnal Studi Komunikasi dan Media, 24(1), 37. https://doi.org/10.31445/jskm.2020.2945.

Kholis, I. M. (2024). Perlindungan data pribadi dan keamanan siber di sektor perbankan: Studi kritis atas penerapan UU PDP dan UU ITE di Indonesia. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4(2), 275–299. https://doi.org/10.14421/t5sfe747.

Krahmann, Elke. (2003). Conceptualizing Security Governance. *Cooperation and Conflict* 38 (1): 5–26. https://doi.org/10.1177/0010836703038001001.

Kristianti, N., & Kurniasi, R. (2024). Peraturan dan regulasi keamanan siber di era digital. Satya Dharma: Jurnal Ilmu Hukum, 7(1). https://ejournal.iahntp.ac.id/index.php/satya-dhamat.

Liebetrau, T., & Bueger, C. (2024). Advancing Coordination in Critical Maritime Infrastructure Protection: Lessons from Maritime Piracy and Cybersecurity. *International Journal of Critical Infrastructure Protection* 46 (September): 100683. https://doi.org/10.1016/j.ijcip.2024.100683.

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi penanganan keamanan siber (cyber security) di Indonesia. Jurnal Review Pendidikan dan Pengajaran, 6(4), 1941–1949. http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/21041

Makbul, M., & Ismail, M. (2023). Kebijakan cyber defend Indonesia dalam rangka menangani international cyber threats. Jurnal Yustitia, 23(2). https://doi.org/10.53712/yustitia.v23i2.1703.

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi: *Politeia: Jurnal Ilmu Politik* 14 (1): 54–62. https://doi.org/10.32734/politeia.v14i1.6351.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE Publications.

Mustikasari, W., Dohamid, A. G., & Cempaka, F. G. (2025). Strategi pertahanan non konvensional Indonesia dalam menangkal ancaman siber asimetris: Studi kasus serangan terhadap infrastruktur kritis. AURELIA: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia, 4(1), 1537–1544.

Nieles, Michael, Kelley Dempsey, and Victoria Yan Pillitteri. (2017). *An Introduction to Information Security*. NIST SP 800-12r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1.

Nuha, M. A. U., Windarta, S., & Salman, M. (2025). NSOC-VM: Kerangka kerja manajemen kerentanan pada National Security Operation Center. Jurnal Teknologi Informasi dan Ilmu Komputer, 12(6), 1291–1302. https://doi.org/10.7454/jkskn.v7i1.10086.

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi implementasi kebijakan pembentukan tim tanggap insiden siber pada sektor pemerintah. Matra Pembaruan, 6(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14.

Rahman, F. N. (2024). Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di Indonesia. *Al-Bahts: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 8–16. https://doi.org/10.32520/albahts.v2i1.3044.

Rahakbauw, I. K., & Batubara, I. A. (2024). Analisis potensi ancaman siber pada bidang ekonomi di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 7(1). https://doi.org/10.7454/jkskn.v7i1.10089.

Ramdhan, T. W., Florina, I. D., & Permadi, D. (2024). Analisis framing pemberitaan peretasan Pusat Data Nasional (PDN) di media online Tempo.co. Journal of Education Research, 5(3), 3368–3379. https://doi.org/10.37985/jer.v5i3.1491.

Ramadhani, N. D., Putra, W. H. N., & Herlambang, A. D. (2020). Evaluasi keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 4(5), 1490–1498.

Rizki, M. (2022). Perkembangan sistem pertahanan/keamanan siber Indonesia dalam menghadapi tantangan perkembangan teknologi dan informasi. Politeia: Jurnal Ilmu Politik, 14(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351.

Sawlani, D. K., & Supriyadi, A. A. (2024). Bridging public policy and defense strategy to combat hybrid warfare: An analytical study on national security. International Journal of Social Service and Research, 4(06), 1834–1842. https://doi.org/10.55324/ijssr.v4i06.820.

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada data PDN: Implikasi etis dan tanggung jawab profesional dalam pengelolaan

keamanan siber. Jurnal Sains Student Research (JSSR), 2(6), 324–331. https://doi.org/10.61722/jssr.v2i6.2966.

Socquet-Clerc, C., Sacks, J., & Kim, J. (2025). *Cybersecurity governance in Southeast Asia: Regional frameworks, national strategies, and capacity building*. Hinrich Foundation. https://www.hinrichfoundation.com/research/wp/cybersecurity-governance-southeast-asia/.

Srilaksmi, N. K. T., Irnadianis, B., Estiningtyas, D., Delareiza, M., Sulistiowati, & Nilam, A. (2023). State defense: Challenges towards digitalization. Journal of Digital Law and Policy, 2(2), 79–92. https://doi.org/10.58982/jdlp.v2i2.313.

Sunkpho, J., Ramjan, S., & Chaisricharoen, R. (2025). Cybersecurity policy in ASEAN countries: A comparative analysis of frameworks and readiness. *International Journal of Critical Infrastructure Protection*, *48*, Article 100642. https://doi.org/10.1016/j.ijcip.2025.100642.

Sutikno, T., & Stiawan, D. (2022). Cyberattacks and Data Breaches in Indonesia by Bjorka: Hacker or Data Collector?. *Bulletin of Electrical Engineering and Informatics* 11 (6): 2989–94. https://doi.org/10.11591/eei.v11i6.4854.

Taufik, A. F. (2021). Indonesia's cyber diplomacy strategy as a deterrence means to face the threat in the Indo-Pacific region. *Journal of Physics: Conference Series*, 1721(1), 012048. https://doi.org/10.1088/1742-6596/1721/1/012048.

Tobondo, Y. A., Juliana, S. F., Ruagadi, H. A., Tondowala, S. F. H., & Ngguna, Y. (2024). Analysis of cybersecurity implementation in Indonesia based on the framework of administrative law. *Interdisciplinary Journal (IDe)*, 2(2), 83–94. https://doi.org/10.61254/idejournal.v2i2.55.

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x.

Wardana, A., Gunaryo, G., & Yogaswara, Y. H. (2022). Development of Cyber Weapons to Improve Indonesia's Cyber Security. *Journal of Social Science* 3 (3): 453–59. https://doi.org/10.46799/jss.v3i3.334.

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak cyber crime terhadap keamanan nasional dan strategi penanggulangannya: Ditinjau dari penegakan hukum. Innovative: Journal Of Social Science Research, 4(3), 15935–15945. https://doi.org/10.31004/innovative.v4i3.11475.

Webber, M., Croft, S., Howorth, J., Terriff, T., & Krahmann, E. (2004). The Governance of European Security. *Review of International Studies* 30 (1): 3–26. https://doi.org/10.1017/S0260210504005807.

Wibowo, S. E., Hartono, A., Kiswanto, H., Primawanti, H., & Louerenss, J. T. A. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. Global Political Studies Journal, 8(2), 97–109. https://doi.org/10.34010/gpsjournal.v8i2.

Witjaksono, D. K., & Kriswibowo, A. (2023). Fondasi keamanan siber untuk layanan pemerintah. Al-Ijtima`i: International Journal of Government and Social Science, 9(1), 21–38. https://doi.org/10.22373/jai.v9i1.2057.

World Economic Forum. (2025). *Global cybersecurity outlook 2025* (Insight Report). WEF. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). Analisis potensi dan strategi pencegahan cyber crime dalam sistem logistik di era digital. *Jurnal Bisnis, Logistik dan Supply Chain (BLOGCHAIN)*, 3(1), 23–32. https://doi.org/10.55122/blogchain.v3i1.714.

Yuryna Connolly, Lena, David S. Wall, Michael Lang, and Bruce Oddson. 2020. “An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability.” *Journal of Cybersecurity* 6 (1): tyaa023. https://doi.org/10.1093/cybsec/tyaa023.