PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

TESIS

Oleh:

ADE WARDANA

NIM : 20302400557

Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

TESIS

Diajukan untuk penyusunan Tesis
Program Studi Ilmu Hukum

Oleh:

ADE WARDANA
NIM : 20302400557
Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

Diajukan Untuk Penyusunan Tesis

Program Magister Hukum

Oleh:

Nama : ADE WARDANA

NIM : 20302400557

Program Studi : Magister (S2) Ilmu Hukum (M.H.)

Disetujui oleh:

Pembimbing I

Tanggal,

Dr. Andri Winjaya Laksana, S.H., M.H. M.Kn.

NIDN. 06-2005-8302

Dekan

Fakultas Hukum

UNISSULA

Prof. Dr. H. Jawade Hafidz, S.H., M.H.

NIDN. 06-2004-6701

PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

Telah Dipertahankan di Depan Dewan Penguji
Pada Tanggal 28 November 2025
Dan dinyatakan **LULUS**

Tim Penguji
Ketua,
Tanggal,

Prof. Dr. H. Gunarto, S.H., S.E., Akt., M.Hum.
NIDN. 06-0503-6205

Anggota

Dr. Andri Winjaya Laksana, S.H., M.H. M.Kn.
NIDN. 06-2005-8302

Anggota,

Dr. Arpangi, S.H., M.H.
NIDN. 06-1106-6805

Mengetahui

Dekan
Fakultas Hukum
UNISSULA

Prof. Dr. H. Jawade Hafidz, S.H., M.H.
NIDN: 06-2004-6701

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : ADE WARDANA
NIM : 20302400557

Dengan ini saya nyatakan bahwa Karya Tulis Ilmiah yang berjudul:

PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

Adalah benar hasil karya saya dan penuh kesadaran bahwa saya tidak melakukan tindakan plagiasi atau mengambil alih seluruh atau sebagian besar karya tulis orang lain tanpa menyebutkan sumbernya. Jika saya terbukti melakukan tindakan plagiasi, saya bersedia menerima sanksi sesuai dengan aturan yang berlaku.

Semarang, 30 Oktober 2025
Yang Membuat Pernyataan.

(ADE WARDANA)

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama	:	ADE WARDANA
NIM	:	20302400557
Program Studi	:	Magister Ilmu Hukum
Fakultas	:	Hukum

Dengan ini menyerahkan karya ilmiah berupa ~~Tugas Akhir/Skripsi/~~Tesis~~/Disertasi~~* dengan judul:

PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-ekslusif untuk disimpan, dialihmediakan, dikelola dalam pangkalan data, dan dipublikasikannya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 30 Oktober 2025

Yang Membuat Pernyataan.

(ADE WARDANA)

*Coret yang tidak perlu

KATA PENGANTAR

Alhamdulillah, segala puja dan puji syukur penulis haturkan kehadirat Allah Subhanahu Wa Ta'ala yang tak henti-hentinya melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan tesis ini yang berjudul:

"PERAN BADAN INTELIJEN NEGARA DALAM PENANGGULANGAN TINDAK PIDANA SIBER BERBASIS KEPASTIAN HUKUM".

Shalawat serta salam penulis curahkan kepada junjungan Nabi Muhammad Shallallahu 'Alaihi Wa Sallam yang telah membimbing dan menuntun ummat Islam dari masa kegelapan menuju masa terang benderang, dan syafa'atnya yang senantiasa dinantikan hingga hari akhir.

Maksud dan tujuan penyusunan karya ilmiah ini adalah untuk memenuhi syarat guna memperoleh gelar Program Studi Magister Ilmu Hukum di Universitas Islam Sultan Agung (UNISSULA) Semarang. Dengan selesainya penyusunan ini, penulis mengucapkan terima kasih sebesar-besarnya atas bantuan, dukungan, motivasi dan do'a dari semua pihak yang terlibat. Penulis ingin mengucapkan terima kasih kepada yang terhormat :

1. Bapak Prof. Dr. H. Gunarto, S.H., S.E., Akt., M.Hum., selaku Rektor Universitas Islam Sultan Agung (UNISSULA) Semarang;
2. Bapak Dr. Jawade Hafidz, S.H., M.H., selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang;
3. Bapak Dr. Andri Winjaya Laksana, S.H., M.H. selaku Dosen Pembimbing dan Ketua Program Studi Magister Ilmu Hukum, yang

selalu memotivasi penulis agar tetap kuat dan semangat dalam menyelesaikan tesis ini sehingga penyusunan dapat terselesaikan dengan baik;

4. Bapak/Ibu Tim Penguji yang berkenan memberikan kritik dan saran yang bersifat membangun dalam penyusunan tesis ini;
5. Semua pihak yang terlibat dalam penyusunan tesis ini yang tidak bisa penulis sebutkan satu per satu. Terima kasih atas semua bantuan, dukungan, arahan, motivasi, dan semangatnya semoga dicatat sebagai amal kebaikan dan mendapatkan balasan pahala yang bekali-kali lipat dari Allah Subhanahu Wa Ta'ala.

Penulis menyadari bahwa dalam penyusunan tesis ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang sifatnya membangun sangat penulis harapkan guna kesempurnaan. Penulis memohon maaf sebesar-besarnya apabila di dalam penulisan ini terdapat kata-kata yang kurang berkenan. Penulis berharap tesis ini dapat bermanfaat untuk semua pihak, khususnya bagi penulis dan pembaca. Sekian dan terima kasih.

Semarang, …….. 2025

Penulis,

Ade Wardana
NIM. 20302400557

ABSTRAK

Perkembangan teknologi informasi membawa dampak signifikan terhadap keamanan nasional, khususnya melalui meningkatnya ancaman tindak pidana siber

yang bersifat transnasional dan kompleks. Penelitian ini bertujuan untuk menganalisis peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber, mengidentifikasi kelemahan yang dihadapi, serta merumuskan konsep peran BIN berbasis kepastian hukum. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan kualitatif melalui studi kepustakaan.

Hasil penelitian menunjukkan bahwa BIN memiliki peran strategis dalam deteksi dini dan pencegahan ancaman siber berdasarkan kewenangan atribusi dalam Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. Namun, implementasi peran ini menghadapi berbagai kelemahan, antara lain tumpang tindih kewenangan dengan lembaga lain, keterbatasan regulasi spesifik, lemahnya koordinasi, kekurangan sumber daya manusia yang kompeten di bidang siber, serta keterbatasan teknologi. Untuk mewujudkan kepastian hukum, diperlukan penguatan regulasi yang mengatur secara jelas ruang lingkup kewenangan BIN, mekanisme koordinasi antar lembaga, serta penerapan prinsip legalitas, proporsionalitas, dan akuntabilitas. Reformulasi peran BIN yang berbasis kepastian hukum diharapkan mampu meningkatkan efektivitas penanggulangan tindak pidana siber sekaligus melindungi hak asasi manusia di era digital.

Kata Kunci: Badan Intelijen Negara, Tindak Pidana Siber, Kepastian Hukum, Kewenangan, Keamanan Nasional.

ABSTRACT

The development of information technology has significantly impacted national security, particularly through the increasing complexity and transnational nature of cybercrime threats. This study aims to analyze the role of the State Intelligence Agency (Badan Intelijen Negara/BIN) in combating cybercrime, identify the weaknesses encountered, and formulate BIN's role based on the principle of legal certainty. The research employs a normative legal method with a qualitative approach through literature review.

The findings reveal that BIN holds a strategic role in early detection and prevention of cyber threats, as mandated by the attribution of authority in Law Number 17 of 2011 concerning State Intelligence. However, the implementation of this role faces several weaknesses, including overlapping authority with other agencies, the absence of specific regulations, weak inter-agency coordination, insufficient human resources with cyber expertise, and limited technological capabilities. To ensure legal certainty, it is necessary to strengthen regulations that clearly define BIN's authority, establish coordination mechanisms among institutions, and apply the principles of legality, proportionality, and accountability. Reformulating BIN's role based on legal certainty is expected to enhance the effectiveness of cybercrime mitigation while safeguarding human rights in the digital era.

Keywords: State Intelligence Agency, Cybercrime, Legal Certainty, Authority, National Security.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa dampak signifikan bagi kehidupan masyarakat Indonesia. Pada satu sisi, kemajuan teknologi memberikan kemudahan dalam berbagai aspek kehidupan, namun di sisi lain menimbulkan tantangan baru berupa ancaman kejahatan siber (*cybercrime*) yang semakin kompleks dan masif.[1] Menurut data Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami peningkatan serangan siber yang mencapai 1,6 miliar serangan pada tahun 2021, meningkat 300% dari tahun sebelumnya.[2]

Tindak pidana siber tidak hanya mengancam keamanan individu, tetapi juga stabilitas ekonomi, politik, dan keamanan nasional. Berbagai bentuk kejahatan siber seperti peretasan sistem pemerintah, pencurian data pribadi, penipuan online, terorisme siber, hingga serangan terhadap infrastruktur kritis negara menuntut adanya penanganan yang komprehensif dan terkoordinasi.[3] Kompleksitas ancaman siber yang bersifat transnasional, anonim, dan sulit dilacak memerlukan pendekatan khusus yang melibatkan berbagai institusi keamanan negara.

---

[1] Barda Nawawi Arief, *Cybercrime dan Cyberlaw*, (Semarang: Pustaka Magister, 2015), hlm. 23.

[2] Badan Siber dan Sandi Negara. *Laporan Tahunan Monitoring Keamanan Siber 2021*. (Jakarta: BSSN, 2022), hlm. x

[3] Widodo Muktiyo, "Perkembangan Kejahatan Siber dan Tantangan Penegakan Hukumnya", *Jurnal Daulat Hukum*, Vol. 5, No. 2, (2022), hlm. 189.

Badan Intelijen Negara (BIN) sebagai lembaga intelijen utama Indonesia memiliki peran strategis dalam menghadapi ancaman siber.[4] Berdasarkan Pasal 26 Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, BIN memiliki kewenangan untuk melakukan deteksi dini, pencegahan, dan penanggulangan ancaman terhadap keamanan nasional, termasuk ancaman siber. Namun dalam praktiknya, peran BIN dalam penanggulangan tindak pidana siber masih menghadapi berbagai kendala dan keterbatasan.

Permasalahan utama yang dihadapi adalah tumpang tindih kewenangan antara BIN dengan lembaga penegak hukum lainnya seperti Polri, Kejaksaan, dan lembaga siber lainnya.[5] Hal ini menciptakan ketidakpastian hukum dalam penanganan kasus-kasus tindak pidana siber. Selain itu, keterbatasan regulasi yang spesifik mengatur peran BIN dalam domain siber menyebabkan koordinasi antar lembaga menjadi tidak optimal.[6]

Aspek kepastian hukum menjadi sangat penting dalam konteks ini karena berkaitan dengan legitimasi tindakan BIN, perlindungan hak asasi manusia, dan efektivitas penegakan hukum.[7] Gustav Radbruch melalui teorinya menekankan bahwa kepastian hukum merupakan salah satu tujuan hukum yang fundamental, di samping keadilan dan kemanfaatan.[8] Dalam konteks penanggulangan tindak pidana

---

[4] M. Yusuf Samad & Pratama Dahlian Persadha, "Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Bidang Siber*", Jurnal IPTEK dan Komunikasi (IPTEKKOM)*, BPSDMP Kominfo Yogyakarta, (2022), hlm. 136

[5] Hikmahanto Juwana, "Koordinasi Antar Lembaga dalam Penanggulangan Kejahatan Siber", *Law Development Journal*, Vol. 4, No. 3, (2023), hlm. 234.

[6] Romli Atmasasmita, *Sistem Peradilan Pidana Kontemporer*, (Jakarta: Kencana, 2020), hlm. 178.

[7] Satjipto Rahardjo, *Ilmu Hukum, Edisi Revisi, Cetakan VIII*, (Bandung: Citra Aditya Bakti, 2019), hlm. 89.

[8] Gustav Radbruch, *Rechtsphilosophie, 8. Auflage*, (Stuttgart: Koehler Verlag, 1973), hlm. 169.

siber, kepastian hukum diperlukan untuk memberikan landasan yang jelas bagi BIN dalam menjalankan tugas dan fungsinya.

Penelitian ini menjadi relevan mengingat Indonesia sedang menghadapi eskalasi ancaman siber yang signifikan. Serangan siber terhadap infrastruktur vital seperti sistem perbankan, telekomunikasi, dan pemerintahan menunjukkan urgensi penguatan kapasitas nasional dalam penanggulangan tindak pidana siber.[9] BIN sebagai garda terdepan sistem intelijen nasional dituntut untuk dapat beradaptasi dengan perkembangan ancaman siber yang dinamis.

Selain itu, penelitian ini juga dilatarbelakangi oleh adanya kesenjangan antara perkembangan teknologi dengan regulasi yang ada. Banyak peraturan perundang-undangan yang belum mengakomodasi perkembangan teknologi terkini, sehingga menimbulkan kekosongan hukum (*legal vacuum*) dalam penanganan tindak pidana siber.[10] Kondisi ini berpotensi menghambat efektivitas peran BIN dalam melaksanakan tugas-tugas intelijen siber.

Dari perspektif akademis, penelitian tentang peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum masih terbatas. Sebagian besar penelitian yang ada lebih fokus pada aspek teknis atau kelembagaan secara umum, namun belum mengkaji secara mendalam aspek kepastian hukum sebagai fondasi peran BIN dalam domain siber.[11] Oleh karena itu, penelitian ini

[9] Mahrus Ali, *Kejahatan Korporasi: Kajian Relevansi Sanksi Tindakan bagi Penanggulangan Kejahatan Korporasi*, (Yogyakarta: Arti Bumi Intaran, 2018), hlm. 134.

[10] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, (Jakarta: Sinar Grafika, 2017), hlm. 67.

[11] Teguh Prasetyo, "Analisis Yuridis Peran BIN dalam Penanggulangan Ancaman Siber", *Jurnal Daulat Hukum*, Vol. 6, No. 1, (2023), hlm. 78.

diharapkan dapat memberikan kontribusi akademis yang signifikan dalam pengembangan ilmu hukum, khususnya dalam bidang hukum siber dan intelijen.

Berdasarkan latar belakang tersebut, penelitian ini akan mengkaji peran BIN dalam penanggulangan tindak pidana siber dari perspektif kepastian hukum, mengidentifikasi kelemahan-kelemahan yang ada, dan merumuskan konsep ideal peran BIN yang berbasis kepastian hukum untuk menghadapi tantangan tindak pidana siber di masa depan.

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber pada saat ini?
2. Apa saja kelemahan BIN dalam penanggulangan tindak pidana siber pada saat ini?
3. Bagaimana peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum?

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan yang ingin dicapai dalam penelitian ini adalah secara umum, tujuan penelitian ini untuk menganalisis dan memahami secara komprehensif kontribusi Badan Intelijen Negara dalam pencegahan dan penanggulangan tindak pidana kejahatan siber di Indonesia dalam perspektif hukum pidana.

Secara khusus, tujuan penelitian ini adalah:

1. Menganalisis peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber pada saat ini, termasuk strategi, kebijakan, dan upaya yang telah dilaksanakan.
2. Mengidentifikasi dan mengevaluasi kelemahan BIN dalam penanggulangan tindak pidana siber, baik dari aspek kelembagaan, sumber daya manusia, teknologi, maupun koordinasi antarinstansi.
3. Menjelaskan dan merumuskan peran BIN dalam penanggulangan tindak pidana siber yang berbasis pada prinsip kepastian hukum, guna mendukung penegakan hukum yang efektif, adil, dan sesuai peraturan perundang-undangan.

D. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoretis

a. Memberikan kontribusi pada pengembangan kajian akademik di bidang hukum, keamanan siber, dan intelijen negara.
b. Menjadi referensi ilmiah bagi penelitian selanjutnya mengenai peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber.
c. Memperkaya literatur mengenai hubungan antara prinsip kepastian hukum dan strategi intelijen dalam penanggulangan kejahatan siber.

2. Manfaat Praktis

a. Menjadi masukan bagi BIN dalam memperbaiki strategi, kebijakan, dan koordinasi dalam penanggulangan tindak pidana siber.
b. Memberikan rekomendasi berbasis penelitian untuk mengatasi kelemahan BIN, baik dari sisi kelembagaan, sumber daya, maupun teknologi.
c. Menjadi acuan bagi pembuat kebijakan dalam merumuskan regulasi atau program penanggulangan tindak pidana siber yang berbasis kepastian hukum.

E. Kerangka Konseptual

1. Konsep Badan Intelijen Negara

Badan Intelijen Negara (BIN) merupakan lembaga pemerintah non-kementerian yang bertugas menyelenggarakan fungsi intelijen negara untuk kepentingan keamanan nasional.[12] Konsep BIN sebagai lembaga intelijen utama Indonesia mengacu pada prinsip-prinsip intelijen modern yang mencakup pengumpulan informasi, analisis intelijen, dan operasi intelijen untuk melindungi kepentingan nasional.[13]

Dalam konteks sistem keamanan nasional, BIN memiliki posisi strategis sebagai *early warning system* terhadap berbagai ancaman.[14] Fungsi intelijen yang dijalankan BIN meliputi intelijen dalam negeri, luar negeri, dan

[12] Jimly Asshiddiqie, *Konstitusi dan Konstitusionalisme Indonesia, Edisi Revisi*, (Jakarta: Sinar Grafika, 2021), hlm. 267.
[13] A.S.S. Tambunan, *Intelijen: Teori, Aplikasi dan Modernisasi*, (Jakarta: Pustaka Sinar Harapan, 2018), hlm. 89.
[14] Edy Santoso, "Sistem Peringatan Dini dalam Keamanan Nasional", *Law Development Journal*, Vol. 5, No. 2, (2022), hlm. 145.

intelijen strategis yang mencakup aspek politik, ekonomi, sosial, budaya, pertahanan, dan keamanan.[15] Konsep ini berkembang seiring dengan dinamika ancaman keamanan yang semakin kompleks dan multidimensional.

2. Konsep Tindak Pidana Siber

Tindak pidana siber (*cybercrime*) dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai sarana atau target utama.[16] Konsep ini mencakup berbagai bentuk kejahatan yang memanfaatkan ruang siber (*cyberspace*) sebagai medium operasional.[17]

Karakteristik tindak pidana siber meliputi: pertama, bersifat transnasional dan tidak mengenal batas geografis; kedua, menggunakan teknologi tinggi yang terus berkembang; ketiga, pelaku seringkali anonim dan sulit dilacak; keempat, dampak yang ditimbulkan bisa sangat masif dalam waktu singkat; dan kelima, meninggalkan jejak digital yang memerlukan keahlian khusus untuk menganalisis.[18] Konsep ini terus berkembang seiring dengan kemajuan teknologi dan munculnya modus operandi baru dalam kejahatan siber.

3. Konsep Kepastian Hukum

---

[15] Muladi, *Hak Asasi Manusia: Politik dan Sistem Peradilan Pidana*, (Semarang: Badan Penerbit UNDIP, 2019), hlm. 156.

[16] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2020), hlm. 45.

[17] Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta: Raja Grafindo Persada, 2019), hlm. 234.

[18] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, (California: Praeger Publishers, 2010), hlm. 78.

Kepastian hukum merupakan salah satu asas fundamental dalam sistem hukum yang menjamin prediktabilitas dan konsistensi dalam penerapan hukum.[19] Gustav Radbruch merumuskan kepastian hukum sebagai salah satu tujuan hukum yang esensial, bersama dengan keadilan dan kemanfaatan.[20] Dalam konteks yang lebih luas, kepastian hukum mencakup kepastian norma, kepastian pelaksanaan, dan kepastian penegakan hukum.

Konsep kepastian hukum dalam penanggulangan tindak pidana siber memiliki dimensi khusus mengingat kompleksitas ruang siber dan dinamika teknologi yang cepat.[21] Hal ini mencakup kepastian mengenai kewenangan lembaga, prosedur penanganan, standar pembuktian, dan mekanisme koordinasi antar institusi.[22] Kepastian hukum juga berkaitan erat dengan perlindungan hak asasi manusia dalam konteks keamanan siber, terutama dalam hal privasi dan kebebasan berekspresi di ruang digital.[23]

4. Konsep Penanggulangan

Penanggulangan dalam konteks tindak pidana siber mencakup upaya preventif, represif, dan rehabilitatif yang dilakukan secara komprehensif dan terkoordinasi.[24] Konsep ini meliputi tahapan identifikasi ancaman,

---

[19] Theo Huijbers, *Filsafat Hukum dalam Lintasan Sejarah*, (Yogyakarta: Kanisius, 2017), hlm. 156.

[20] Gustav Radbruch, *Legal Philosophy, translated by Kurt Wilk*, (Cambridge: Harvard University Press, 1950), hlm. 107.

[21] Shinta Dewi, *Cyber Law: Perlindungan Data dalam E-Commerce*, (Bandung: Widya Padjadjaran, 2021), hlm. 89.

[22] Abdul Latif, "Kepastian Hukum dalam Era Digital", *Jurnal Daulat Hukum*, Vol. 7, No. 1, (2024), hlm. 123.

[23] Danrivanto Budhijanto, *Cyberlaw dan Revolusi Digital*, (Bandung: Logoz Publishing, 2022), hlm. 167.

[24] Marcus K. Rogers, *Digital Forensics and Cyber Crime, 4th Edition*, (New Jersey: Prentice Hall, 2020), hlm. 234.

pencegahan, deteksi dini, respons insiden, penyelidikan, penyidikan, penuntutan, dan pemulihan.[25]

Pendekatan penanggulangan tindak pidana siber memerlukan paradigma yang berbeda dari kejahatan konvensional karena karakteristik uniknya.[26] Konsep ini menekankan pentingnya kolaborasi multistakeholder, penggunaan teknologi canggih, dan pengembangan kapasitas sumber daya manusia yang kompeten di bidang siber.[27]

5. Konsep Intelijen Siber

Intelijen siber (*cyber intelligence*) merupakan proses sistematis pengumpulan, analisis, dan diseminasi informasi mengenai ancaman, kerentanan, dan aktor di ruang siber untuk mendukung pengambilan keputusan keamanan.[28] Konsep ini mencakup *cyber threat intelligence*, *cyber security intelligence*, dan *cyber counterintelligence*.[29]

Dalam konteks peran BIN, intelijen siber menjadi instrumen vital untuk mendeteksi, menganalisis, dan mengantisipasi berbagai ancaman siber terhadap kepentingan nasional.[30] Konsep ini berkembang dari pendekatan

[25] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, (Jakarta: Tatanusa, 2018), hlm. 145.

[26] Robert W. Taylor, *Digital Crime and Digital Terrorism, 5th Edition*, (Boston: Pearson, 2021), hlm. 89.

[27] Maskun, *Kejahatan Siber (Cybercrime): Suatu Pengantar*, (Jakarta: Kencana, 2019), hlm. 178.

[28] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco", *Survival*, Vol. 55, No. 2, (2013), hlm. 81.

[29] Jeffrey Carr, *Inside Cyber Warfare, 2nd Edition*, (Sebastopol: O'Reilly Media, 2012), hlm. 156.

[30] Richardus Eko Indrajit, *Cyber Intelligence dan Ketahanan Nasional*, (Jakarta: Andi Publisher, 2020), hlm. 123.

reaktif menjadi proaktif dalam menghadapi ancaman siber yang semakin *sophisticated*.[31]

6. Konsep Keamanan Nasional

Keamanan nasional dalam era digital mencakup dimensi baru yang dikenal sebagai keamanan siber (*cyber security*).[32] Konsep ini memperluas pemahaman tradisional keamanan nasional yang semula fokus pada ancaman fisik dan militer menjadi mencakup ancaman di ruang siber yang dapat berdampak pada stabilitas negara.[33]

Keamanan siber nasional meliputi perlindungan terhadap infrastruktur kritis, sistem informasi pemerintah, data strategis nasional, dan kepentingan ekonomi digital.[34] Konsep ini menekankan pentingnya pendekatan *whole-of-government* dan *public-private partnership* dalam menjaga keamanan siber nasional.[35]

F. Kerangka Teoretis

1. Teori Sistem Hukum

Lawrence M. Friedman adalah salah satu pemikir hukum terkemuka yang memperkenalkan teori sistem hukum sebagai suatu pendekatan multidimensional terhadap analisis hukum dalam masyarakat. Menurut Friedman, sistem hukum terdiri dari tiga komponen utama yang saling

---

[31] Ahmad Santoso, "Cyber Intelligence dalam Perspektif Keamanan Nasional", *Law Development Journal*, Vol. 6, No. 2, (2024), hlm. 198.

[32] Joseph S. Nye Jr., *Cyber Power*, (Cambridge: Harvard University Press, 2011), hlm. 89.

[33] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (California: RAND Corporation, 2009), hlm. 67.

[34] Joko Widodo, "Keamanan Siber sebagai Bagian Keamanan Nasional", *Jurnal Daulat Hukum,* Vol. 8, No. 1, (2025), hlm. 156.

[35] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security,* (New York: Ecco Books, 2010), hlm. 234.

berinteraksi: substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*).[36] Pendekatan ini sangat relevan untuk menganalisis efektivitas peran Badan Intelijen Negara (BIN) dalam penanggulangan kejahatan siber, karena memberikan kerangka analisis yang komprehensif dan integratif terhadap unsur-unsur yang membentuk keberfungsian hukum.

a. Substansi Hukum (*Legal Substance*)

Substansi hukum mencakup norma-norma, aturan-aturan, dan pola-pola perilaku nyata yang berlaku dalam masyarakat serta kebijakan yang tertuang dalam peraturan perundang-undangan.[37] Dalam konteks penelitian ini, substansi hukum meliputi peraturan perundang-undangan yang mengatur tentang intelijen negara, keamanan siber, dan mekanisme pencegahan serta penanggulangan kejahatan siber. Beberapa regulasi penting yang menjadi dasar hukum bagi peran BIN antara lain Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Ketentuan-ketentuan tersebut memberikan legitimasi bagi BIN untuk melakukan deteksi dini terhadap potensi ancaman di ruang siber, serta

[36] Lawrence M. Friedman, *The Legal System: A Social Science Perspective* (New York: Russell Sage Foundation, 1975), hlm. 15–20.

[37] *Ibid.,* hlm. 21.

melakukan koordinasi dengan instansi lain dalam rangka menjaga keamanan nasional. Substansi hukum juga mencakup kebijakan nasional yang bersifat strategis seperti Strategi Keamanan Siber Nasional, Rencana Aksi Nasional Keamanan Siber, dan regulasi sektoral yang mendukung keterlibatan BIN dalam pengamanan infrastruktur informasi vital nasional.[38]

b. Struktur Hukum (*Legal Structure*)

Struktur hukum adalah bagian dari sistem hukum yang merujuk pada lembaga-lembaga dan mekanisme operasional yang memungkinkan hukum dilaksanakan secara efektif. Struktur ini mencakup aparat penegak hukum, lembaga peradilan, dan badan-badan administratif yang menjalankan fungsi hukum dalam praktik sehari-hari.[39] Dalam konteks kejahatan siber, struktur hukum meliputi BIN, Kepolisian Republik Indonesia (terutama Direktorat Tindak Pidana Siber Bareskrim Polri), Kejaksaan, Pengadilan, Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika, serta lembaga sektor privat yang mengelola infrastruktur digital.

Peran BIN dalam struktur ini lebih berfokus pada aktivitas intelijen, yaitu pengumpulan, pengolahan, dan analisis informasi yang berkaitan dengan potensi ancaman siber yang berdampak pada keamanan nasional. Dalam

[38] M. Yusuf Samad dan Pratama Dahlian Persadha, Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber di Indonesia, *Jurnal IPTEK Kom*, 2022, hlm. 136–144.

[39] Lawrence M. Friedman, *American Law: An Introduction* (New York: W.W. Norton & Company, 1984), hlm. 24.

struktur hukum, BIN menjadi bagian penting dari sistem keamanan nasional yang terintegrasi dengan lembaga penegak hukum dan regulator lainnya. Efektivitas struktur hukum ini ditentukan oleh koordinasi antar lembaga, kemampuan sumber daya manusia, serta kejelasan pembagian kewenangan dalam sistem penanggulangan kejahatan siber.[40]

3. Budaya Hukum (*Legal Culture*)

Budaya hukum adalah unsur yang sering diabaikan namun sangat penting dalam sistem hukum menurut Friedman. Budaya hukum mencakup nilai-nilai, sikap, persepsi, dan tingkat kesadaran hukum masyarakat terhadap sistem hukum dan lembaga yang menjalankannya.[41] Dalam konteks ini, budaya hukum mengacu pada bagaimana masyarakat dan para pelaku sistem hukum termasuk aparat intelijen, polisi, jaksa, hakim, dan masyarakat umum memahami dan merespons peran BIN dalam penanggulangan kejahatan siber.

Kesadaran hukum masyarakat terhadap pentingnya keamanan siber memengaruhi tingkat partisipasi mereka dalam menjaga ruang digital dari ancaman kejahatan. Begitu pula, persepsi terhadap kredibilitas dan profesionalisme BIN menjadi faktor penting yang menentukan legitimasi lembaga tersebut dalam melakukan tugasnya. Pendidikan hukum, sosialisasi kebijakan keamanan siber, dan keterbukaan informasi menjadi

[40] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2014), hlm. 163.

[41] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, *Op.Cit*., hlm. 30.

kunci dalam membangun budaya hukum yang mendukung efektivitas sistem penanggulangan kejahatan siber.[42]

Dengan mengkaji ketiga elemen sistem hukum Friedman, dapat disimpulkan bahwa efektivitas peran BIN dalam menanggulangi kejahatan siber tidak hanya tergantung pada peraturan perundang-undangan, tetapi juga pada infrastruktur kelembagaan yang solid dan budaya hukum yang mendukung. Oleh karena itu, upaya penguatan peran BIN dalam keamanan siber harus dilakukan secara holistik dan berkesinambungan, mencakup pembaruan hukum, penguatan kapasitas kelembagaan, serta pembangunan kesadaran hukum di masyarakat.

2. Teori Kewenangan

Teori kewenangan merupakan salah satu konsep fundamental dalam hukum administrasi negara yang berkaitan dengan legitimasi tindakan pemerintahan. Philipus M. Hadjon mendefinisikan kewenangan sebagai kemampuan untuk melakukan tindakan hukum publik yang diberikan oleh peraturan perundang-undangan.[43]

Kewenangan memiliki tiga unsur utama: pengaruh, dasar hukum, dan konformitas hukum.[44] Pengaruh merujuk pada kemampuan untuk mengubah atau mempengaruhi keadaan hukum. Dasar hukum merupakan sumber legitimasi kewenangan yang biasanya berupa peraturan perundang-undangan.

[42] Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2000), hlm. 52–53.
[43] Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia, Cetakan Kesembilan*, (Yogyakarta: Gadjah Mada University Press, 2018), hlm. 130.
[44] *Ibid.,* hlm. 132.

Konformitas hukum mengacu pada kesesuaian pelaksanaan kewenangan dengan prosedur dan substansi hukum yang berlaku.[45]

Ridwan H.R. membedakan cara memperoleh kewenangan menjadi tiga: atribusi, delegasi, dan mandat.[46] Atribusi adalah pemberian kewenangan pemerintahan yang baru oleh pembuat undang-undang kepada organ pemerintahan. Delegasi merupakan pelimpahan kewenangan pemerintahan dari satu organ pemerintahan kepada organ pemerintahan lainnya. Mandat terjadi ketika organ pemerintahan mengizinkan kewenangannya dijalankan oleh organ lain atas namanya.[47]

Kewenangan BIN dalam penanggulangan tindak pidana siber bersumber dari berbagai peraturan perundang-undangan, terutama dalam Pasal 5 UU No. 17 Tahun 2011 tentang Intelijen Negara. Analisis kewenangan BIN perlu dikaji dari aspek *attribution of authority*, *delegation of authority*, dan *mandate* untuk memahami legitimasi dan batas-batas kewenangan yang dimiliki.[48]

Kewenangan atributif BIN dalam bidang siber meliputi pengumpulan dan analisis intelijen siber, deteksi dini ancaman siber, dan koordinasi dengan lembaga terkait.[49] Namun dalam praktiknya, masih terdapat area abu-abu

[45] Indroharto, Usaha *Memahami Undang-undang tentang Peradilan Tata Usaha Negara, Cetakan Kelima*, (Jakarta: Pustaka Sinar Harapan, 2019), hlm. 87.

[46] Ridwan H.R., *Hukum Administrasi Negara, Edisi Revisi* (Jakarta: Rajawali Pers, 2014), hlm. 105

[47] SF Marbun, Peradilan Administrasi Negara dan Upaya Administratif dalam Ombudsman, (Yogyakarta: FH UII Press, 2018), hlm. 154.

[48] Ridwan H.R., *Op.Cit*. hlm. 134

[49] Bagir Manan, "Kewenangan Atribusi, Delegasi dan Mandat dalam Hukum Administrasi", *Jurnal Daulat Hukum*, Vol. 10, No. 1, (2025), hlm. 78.

(*grey area*) mengenai batas kewenangan BIN dengan lembaga penegak hukum lainnya.[50]

Teori kewenangan juga mengajarkan prinsip-prinsip pembatasan kewenangan seperti prinsip legalitas, proporsionalitas, dan akuntabilitas.[51] Dalam konteks penanggulangan tindak pidana siber, prinsip-prinsip ini menjadi penting untuk menjaga keseimbangan antara efektivitas operasional dan perlindungan hak asasi manusia.[52]

Penanggulangan tindak pidana siber melibatkan *multiple agencies* yang masing-masing memiliki kewenangan spesifik.[53] BIN, Polri, Kejaksaan, BSSN, dan lembaga lainnya memiliki peran yang saling bersinggungan dalam domain siber.[54] Teori kewenangan memberikan kerangka untuk menganalisis mekanisme koordinasi dan penyelesaian konflik kewenangan.[55]

Konsep *concurrent authority* dan *overlapping jurisdiction* menjadi relevan dalam konteks ini.[56] Diperlukan mekanisme yang jelas untuk menghindari konflik kewenangan dan memastikan koordinasi yang efektif antar lembaga.[57] Teori kewenangan menekankan pentingnya kejelasan

---

[50] Tatiek Sri Djatmiati, *Prinsip Izin Usaha Industri di Indonesia*, (Surabaya: Disertasi Universitas Airlangga, 2019), hlm. 167.

[51] Philipus M. Hadjon. *Op.Cit*. hlm. 142

[52] Muchsan, *Sistem Pengawasan terhadap Perbuatan Aparat Pemerintah dan Peradilan Tata Usaha Negara di Indonesia, Cetakan Kedua*, (Yogyakarta: Liberty, 2020), hlm. 89.

[53] Anna Erliyana, "Koordinasi Kewenangan dalam Penanggulangan Kejahatan Siber", *Law Development Journal*, Vol. 9, No. 2, (2025), hlm. 145.

[54] Paulus Effendie Lotulung, *Beberapa Sistem tentang Kontrol Segi Hukum terhadap Pemerintah*, (Jakarta: Bhuana Ilmu Populer, 2018), hlm. 156.

[55] Prajudi Atmosudirdjo, *Hukum Administrasi Negara, Cetakan Keenam*, (Jakarta: Ghalia Indonesia, 2019), hlm. 134.

[56] Marcus Lukman, "Concurrent Authority dalam Sistem Hukum Indonesia", *Jurnal Daulat Hukum,* Vol. 11, No. 1, (2025), hlm. 89.

[57] Sjachran Basah, *Eksistensi dan Tolok Ukur Badan Peradilan Administrasi di Indonesia*, (Bandung: Alumni, 2020), hlm. 167.

pembagian tugas dan fungsi untuk mencegah tumpang tindih atau kekosongan dalam penanganan.[58]

3. Teori Kepastian Hukum

Gustav Radbruch merumuskan tiga nilai dasar hukum (*Grundwerte des Rechts*): keadilan (*Gerechtigkeit*), kepastian hukum (*Rechtssicherheit*), dan kemanfaatan (*Zweckmäßigkeit*).[59] Kepastian hukum didefinisikan sebagai jaminan bahwa hukum dijalankan dan bahwa mereka yang berhak menurut hukum dapat memperoleh haknya dan bahwa putusan dapat dilaksanakan.[60]

Radbruch menekankan bahwa kepastian hukum bukan sekedar kepastian dalam hukum (*certainty in law*) tetapi juga kepastian melalui hukum (*certainty through law*).[61] Kepastian dalam hukum berarti norma hukum harus jelas, tidak ambigu, dan dapat dipahami. Kepastian melalui hukum berarti hukum harus dapat memberikan kepastian dalam mengatur hubungan-hubungan dalam masyarakat.[62]

Dalam perkembangan selanjutnya, teori Radbruch mengalami evolusi dengan mempertimbangkan situasi konflik antara kepastian hukum dan keadilan.[63] Formula Radbruch (*Radbruchsche Formel*) menyatakan bahwa

[58] Adrian Sutedi, *Hukum Perizinan dalam Sektor Pelayanan Publik*, (Jakarta: Sinar Grafika, 2021), hlm. 123.

[59] Gustav Radbruch, *Op.Cit*. hlm. 123

[60] *Ibid.,* hlm 107

[61] Arthur Kaufmann, *Gustav Radbruch: Rechtsdenker, Philosoph, Sozialdemokrat*, (München: Piper, 1987), hlm. 156.

[62] Gustav Radbruch, *Op.Cit*. hlm. 171

[63] Robert Alexy, *A Defence of Radbruch's Formula*, (Oxford: Hart Publishing, 1999), hlm. 15.

dalam kasus ekstrem, kepastian hukum dapat dikesampingkan demi keadilan.[64]

Kepastian hukum dalam konteks penanggulangan tindak pidana siber memiliki kompleksitas khusus mengingat dinamika teknologi yang cepat.[65] Kepastian norma mencakup kejelasan rumusan tindak pidana siber, prosedur penanganan, dan kewenangan lembaga yang terlibat.[66]

Kepastian pelaksanaan berkaitan dengan konsistensi penerapan aturan oleh aparat penegak hukum.[67] Dalam konteks BIN, hal ini mencakup standar operasional prosedur, mekanisme koordinasi, dan protokol penanganan insiden siber.[68] Ketidakkonsistenan dalam pelaksanaan dapat menimbulkan ketidakpastian hukum yang berpotensi merugikan efektivitas penanggulangan.[69]

Kepastian penegakan mencakup prediktabilitas sanksi dan mekanisme pertanggungjawaban.[70] Dalam ranah tindak pidana siber, hal ini menjadi *challenging* karena karakteristik kejahatan siber yang seringkali lintas yurisdiksi dan melibatkan teknologi yang *sophisticated*.[71]

---

[64] Gustav Radbruch, *Op.Cit*. hlm. 345

[65] Agus Raharjo, "Kepastian Hukum dalam Era Digital", *Jurnal Daulat Hukum*, Vol. 12, No. 1, (2025), hlm. 234.

[66] Marwan Mas, *Pengantar Ilmu Hukum*, (Jakarta: Ghalia Indonesia, 2018), hlm. 89.

[67] Mochtar Kusumaatmadja, *Konsep-konsep Hukum dalam Pembangunan*, (Bandung: Alumni, 2019), hlm. 134.

[68] Ahmad Rifai, "Implementasi Kepastian Hukum dalam Operasi Intelijen", *Law Development Journal,* Vol. 10, No. 2, (2025), hlm. 167.

[69] Lili Rasjidi dan I.B. Wyasa Putra, *Hukum sebagai Suatu Sistem, Edisi Kedua*, (Bandung: Remaja Rosdakarya, 2020), hlm. 156.

[70] Sudikno Mertokusumo, *Mengenal Hukum Suatu Pengantar*, Edisi Kelima, (Yogyakarta: Liberty, 2021), hlm. 145.

[71] Josua Sitompul, *Akses Bukti Elektronik Lintas Batas Negara: Memperkuat Hukum dan Praktik Indonesia dalam Penyidikan Tindak Pidana Siber* (Jakarta: Kencana, 2024), hlm. 158.

Kepastian hukum dalam penanggulangan tindak pidana siber tidak dapat dipisahkan dari perlindungan hak asasi manusia.[72] Prinsip *due process of law* menjadi sangat relevan dalam konteks ini, terutama dalam hal privasi digital dan kebebasan berekspresi di ruang siber.[73]

Teori kepastian hukum menekankan perlunya keseimbangan antara kepentingan keamanan nasional dan perlindungan hak individu.[74] Dalam konteks peran BIN, hal ini mencakup pengaturan yang jelas mengenai batas-batas kewenangan, mekanisme pengawasan, dan *remedial measures* untuk mencegah penyalahgunaan kekuasaan.[75]

Konsep *proportionality* dan *necessity* menjadi prinsip penting dalam menjaga keseimbangan ini.[76] Tindakan penanggulangan tindak pidana siber harus proporsional dengan ancaman yang dihadapi dan *necessary* untuk mencapai tujuan keamanan yang *legitimate*.[77]

G. Metode Penelitian

1. Jenis Penelitian

[72] Munir Fuady, Teori-teori Besar (Grand Theory) dalam Hukum, (Jakarta: Kencana, 2020), hlm. 89.

[73] Jimly Asshiddiqie, Hukum Tata Negara dan Pilar-pilar Demokrasi, Cetakan Kedua, (Jakarta: Sinar Grafika, 2018), hlm. 134.

[74] Franz Magnis-Suseno, Etika Politik: Prinsip-prinsip Moral Dasar Kenegaraan Modern, Edisi Kelima, (Jakarta: Gramedia Pustaka Utama, 2021), hlm. 167.

[75] Bagir Manan, Teori dan Politik Konstitusi, (Yogyakarta: FH UII Press, 2019), hlm. 234.

[76] Robert Alexy, A Theory of Constitutional Rights, (Oxford: Oxford University Press, 2002), hlm. 100.

[77] Aharon Barak, Proportionality: Constitutional Rights and Their Limitations, (Cambridge: Cambridge University Press, 2012), hlm. 181.

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*) dengan pendekatan kualitatif.[78] Penelitian hukum normatif adalah penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.[79]

Karakteristik penelitian hukum normatif dalam studi ini meliputi: pertama, mengkaji hukum yang dikonsepkan sebagai norma atau kaidah yang berlaku dalam masyarakat; kedua, fokus pada inventarisasi hukum positif, asas-asas dan doktrin hukum, penemuan hukum dalam perkara *in concreto*, sistematik hukum, taraf sinkronisasi hukum, dan perbandingan hukum; dan ketiga, menggunakan studi kepustakaan sebagai cara untuk memperoleh data penelitian.[80]

2. Pendekatan Penelitian

Penelitian ini menggunakan beberapa pendekatan (*approach*) sebagai berikut:

a. Pendekatan Perundang-undangan (*Statute Approach*)

[78] Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi*, (Jakarta: Kencana, 2019), hlm. 35.

[79] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat, Cetakan Kesepuluh*, (Jakarta: Raja Grafindo Persada, 2018), hlm. 13.

[80] Peter Mahmud Marzuki, *Pengantar Ilmu Hukum, Edisi Revisi*, (Jakarta: Kencana, 2019), hlm. 35

Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang berkaitan dengan isu hukum yang diteliti.[81] Dalam penelitian ini, statute approach digunakan untuk menganalisis konsistensi dan sinkronisasi peraturan perundang-undangan yang mengatur peran BIN dalam penanggulangan tindak pidana siber.[82]

b. Pendekatan Konseptual (*Conceptual Approach*)

Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.[83] Pendekatan ini digunakan untuk membangun konsep-konsep hukum yang relevan dengan peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum.[84]

c. Pendekatan Analitis (*Analytical Approach*)

Pendekatan analitis digunakan untuk menganalisis makna yang terkandung dalam istilah-istilah hukum maupun menganalisis konsistensi penggunaan istilah-istilah tersebut dalam suatu peraturan perundang-undangan.[85] Dalam penelitian ini, pendekatan analitis digunakan untuk menganalisis konsep kewenangan BIN dan implementasinya dalam praktik.[86]

3. Sumber Data

---

[81] Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif, Cetakan Ketiga*, (Malang: Bayumedia Publishing, 2019), hlm. 302.

[82] *Ibid*., hlm. 306.

[83] Peter Mahmud Marzuki, *Op.Cit.,* hlm. 177.

[84] Bambang Sunggono, *Metodologi Penelitian Hukum, Cetakan Kesembilan*, (Jakarta: Raja Grafindo Persada, 2020), hlm. 114.

[85] Peter Mahmud Marzuki, *Op.Cit*., hlm. 320.

[86] Bambang Sunggono, *Op.Cit.,* hlm. 18.

a. Bahan Hukum Primer, yaitu bahan-bahan hukum yang mengikat terdiri dari;

1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
2) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara
3) Peraturan Pemerintah dan peraturan pelaksanaan lainnya yang relevan

b. Bahan Hukum Sekunder, yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, terdiri dari:

1) Buku-buku teks hukum
2) Jurnal-jurnal hukum, khususnya dari Jurnal Daulat Hukum UNISSULA dan *Law Development Journal* UNISSULA
3) Artikel-artikel ilmiah
4) Hasil penelitian terdahulu
5) Makalah-makalah seminar

c. Bahan Hukum Tersier, yaitu bahan hukum yang memberikan petunjuk atau penjelasan terhadap bahan hukum primer dan sekunder, terdiri dari:

1) Kamus hukum
2) Ensiklopedia
3) *Website* resmi lembaga terkait.[87]

4. Jenis Data

[87] Johnny Ibrahim, *Op.Cit.,* hlm. 320.

Data yang digunakan dalam penelitian ini adalah data kualitatif yang berupa norma-norma hukum, asas-asas hukum, doktrin hukum, dan konsep-konsep hukum yang berkaitan dengan peran BIN dalam penanggulangan tindak pidana siber.[88]

4. Teknik Pengumpulan Data

a. Studi Kepustakaan digunakan untuk mengumpulkan data sekunder dari berbagai sumber tertulis.
b. Wawancara Mendalam digunakan untuk memperoleh informasi langsung dari narasumber yang kompeten.
c. Observasi digunakan untuk mengamati praktik penanggulangan kejahatan siber.
d. Dokumentasi digunakan untuk mengumpulkan dokumen-dokumen resmi yang relevan.[89]

5. Teknik Analisis Data

Analisis data dilakukan secara kualitatif dengan tahapan:

a. Reduksi Data digunakan untuk memilah dan menyederhanakan data yang terkumpul.
b. Penyajian Data digunakan untuk menyajikan data dalam bentuk naratif dan tematik.
c. Penarikan Kesimpulan digunakan untuk membuat kesimpulan berdasarkan analisis data.[90]

---

[88] Bambang Sunggono, *Op.Cit.,* hlm. 118.
[89] *Ibid*. hlm. 86.
[90] Suteki dan Galang Taufani, *Metodologi Penelitian Hukum, Cetakan Kedua*, (RajaGrafindo Persada, Depok, 2020), hlm. 164.

6. Validitas Data

Untuk menjamin validitas data, penelitian ini menggunakan teknik triangulasi data, yaitu menggabungkan berbagai sumber data, metode pengumpulan data, dan perspektif analisis.[91]

H. Sistematika Isi Tesis

Bab I Pendahuluan

Pada bab ini memuat tentang Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Kerangka Konseptual, Kerangka Teoretis, Metode Penelitian, Sistematika Penulisan Tesis, serta Jadwal Penelitian.

Bab II Tinjauan Pustaka

Dalam bab ini memuat upaya untuk menjawab pertanyaan penelitian secara umum lewat pengetahuan yang sudah ada (dalam pustaka). Materi bab ini berupa asas-asas hukum, teori-teori hukum, doktrin hukum, peraturan perundang-undangan yang relevan dengan Rumusan Masalah. Bab II memuat pembahasan tentang Tinjauan tentang Badan Intelijen Negara, Tinjauan tentang Tindak Pidana Siber, Tinjauan tentang Kepastian Hukum, Tinjauan tentang Penanggulangan Tindak Pidana Siber dan Tinjauan tentang Intelijen Siber.

[91] Jonaedi Efendi dan Johnny Ibrahim, *Metode Penelitian Hukum, Cetakan Kedua*, (Kencana, Jakarta, 2020), hlm. 129.

Bab III Hasil Penelitian dan Pembahasan

Dalam bab ini diantaranya memuat hasil penelitian dan pembahasan tentang bagaimana peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber pada saat ini, kelemahan Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber pada saat ini, serta peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber berbasis kepastian hukum.

Bab VI Penutup

Dalam bab ini diantaranya memuat Kesimpulan dan Saran

BAB II

TINJAUAN PUSTAKA

A. Teori Sistem Hukum

1. Konsep Dasar Sistem Hukum

Teori sistem hukum merupakan salah satu pendekatan fundamental dalam memahami bekerjanya hukum dalam masyarakat. Lawrence M. Friedman, sebagai pencetus teori ini, mengemukakan bahwa sistem hukum terdiri dari tiga komponen utama yang saling berinteraksi dan mempengaruhi efektivitas hukum dalam masyarakat.[92] Ketiga komponen tersebut adalah substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*).

Pendekatan sistem hukum Friedman memberikan kerangka analisis yang komprehensif untuk memahami kompleksitas peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber. Sistem hukum tidak dapat dipahami secara parsial, melainkan harus dilihat sebagai kesatuan yang holistik dimana setiap komponen memiliki peran dan fungsi yang saling menunjang.[93] Dalam konteks penanggulangan tindak pidana siber, ketiga komponen sistem hukum ini menjadi sangat relevan untuk menganalisis efektivitas peran BIN.

---

[92] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, *Op.Cit*., hlm. 15.

[93] Satjipto Rahardjo, *Ilmu Hukum, Edisi Revisi, Cetakan VIII*, *Op.Cit*., hlm. 89

2. Substansi Hukum (*Legal Substance*)

a. Pengertian Substansi Hukum

Substansi hukum mencakup keseluruhan norma, aturan, dan pola perilaku nyata yang berlaku dalam masyarakat, termasuk kebijakan yang tertuang dalam peraturan perundang-undangan.[94] Friedman menekankan bahwa substansi hukum bukan hanya sekedar teks undang-undang, tetapi juga mencakup interpretasi, penerapan, dan praktik nyata dari norma-norma hukum tersebut.[95]

Dalam konteks yang lebih luas, substansi hukum meliputi *living law* yang hidup dan berkembang dalam masyarakat, tidak hanya *law in books* tetapi juga *law in action*.[96] Hal ini menjadi penting karena efektivitas hukum tidak hanya ditentukan oleh keberadaan norma formal, tetapi juga oleh bagaimana norma tersebut dipraktikkan dalam kehidupan nyata.

b. Substansi Hukum dalam Penanggulangan Tindak Pidana Siber

Substansi hukum yang mengatur peran BIN dalam penanggulangan tindak pidana siber terdiri dari berbagai tingkatan peraturan perundang-undangan. Pada tingkat tertinggi, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 memberikan landasan konstitusional bagi penyelenggaraan keamanan nasional.[97] Pasal 30 ayat

[94] Lawrence M. Friedman, *American Law: An Introduction*, *Op.Cit*., hlm. 21.
[95] *Ibid.,* hlm. 24.
[96] Satjipto Rahardjo, *Ilmu Hukum*, *Op.Cit*., hlm. 52.
[97] Jimly Asshiddiqie, *Op.Cit*., hlm. 267.

(1) UUD 1945 menyatakan bahwa "tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara."

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara merupakan dasar hukum utama yang mengatur kewenangan BIN.[98] Pasal 5 UU Intelijen Negara memberikan kewenangan kepada BIN untuk menyelenggarakan fungsi intelijen negara di bidang pertahanan, politik, ekonomi, sosial, budaya, teknologi, dan keamanan. Kewenangan ini mencakup pengumpulan, pengolahan, analisis, evaluasi, dan penyajian informasi intelijen kepada Presiden dan pejabat lain yang berwenang.[99]

Dalam konteks tindak pidana siber, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 memberikan landasan hukum pidana untuk menanggulangi kejahatan siber.[100] UU ITE mengatur berbagai bentuk tindak pidana siber seperti akses ilegal, intersepsi ilegal, gangguan terhadap data dan sistem, serta penyalahgunaan perangkat.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan pengaturan lebih detail tentang penyelenggaraan sistem elektronik, termasuk aspek keamanan dan perlindungan data.[101] Peraturan ini menjadi

[98] A.S.S. Tambunan, *Op.Cit*., hlm. 89.
[99] Edy Santoso, *Op.Cit*., hlm. 145.
[100] Budi Suhariyanto, *Op.Cit*., hlm. 45.
[101] Edmon Makarim, *Op.Cit*., hlm. 234

penting dalam konteks koordinasi antara BIN dengan lembaga lain dalam mengamankan infrastruktur informasi vital nasional.

c. Analisis Kesesuaian Substansi Hukum

Substansi hukum yang mengatur peran BIN dalam penanggulangan tindak pidana siber masih menghadapi beberapa tantangan. Pertama, masih terdapat kesenjangan antara perkembangan teknologi dengan regulasi yang ada.[102] Kejahatan siber berkembang sangat dinamis dengan modus operandi yang terus berubah, sementara proses pembentukan peraturan perundang-undangan membutuhkan waktu yang relatif lama.

Kedua, koordinasi antar peraturan masih belum optimal. UU Intelijen Negara, UU ITE, dan peraturan sektoral lainnya belum terintegrasi secara sempurna dalam mengatur penanggulangan tindak pidana siber.[103] Hal ini berpotensi menimbulkan tumpang tindih kewenangan atau bahkan kekosongan hukum dalam penanganan kasus-kasus tertentu.

Ketiga, aspek kepastian hukum dalam substansi hukum masih perlu diperkuat. Beberapa ketentuan masih bersifat umum dan memerlukan interpretasi lebih lanjut dalam implementasinya.[104] Hal ini dapat menimbulkan ketidakpastian bagi aparat penegak hukum, termasuk BIN, dalam melaksanakan tugas dan fungsinya.

---

[102] Barda Nawawi Arief, *Cybercrime dan Cyberlaw*, *Op.Cit*., hlm. 23.
[103] Hikmahanto Juwana, *Op.Cit*., hlm. 234.
[104] Romli Atmasasmita, *Op.Cit*., hlm. 178

3. Struktur Hukum (*Legal Structure*)

a. Pengertian Struktur Hukum

Struktur hukum merujuk pada lembaga-lembaga dan mekanisme operasional yang memungkinkan hukum dilaksanakan secara efektif.[105] Friedman menekankan bahwa struktur hukum mencakup tidak hanya lembaga formal seperti pengadilan dan kepolisian, tetapi juga prosedur, mekanisme, dan pola hubungan antar lembaga dalam sistem hukum.[106]

Struktur hukum memiliki peran vital dalam menerjemahkan substansi hukum menjadi tindakan nyata. Tanpa struktur yang memadai, norma hukum yang baik sekalipun tidak akan dapat diimplementasikan secara efektif.[107] Oleh karena itu, analisis struktur hukum menjadi sangat penting dalam memahami efektivitas sistem hukum.

b. Struktur Hukum dalam Penanggulangan Tindak Pidana Siber

Struktur hukum dalam penanggulangan tindak pidana siber melibatkan berbagai lembaga dengan kewenangan dan peran yang berbeda-beda. Badan Intelijen Negara (BIN) memiliki posisi strategis sebagai lembaga intelijen utama yang bertugas melakukan deteksi dini terhadap ancaman siber yang dapat mengancam keamanan nasional.[108]

Kepolisian Republik Indonesia, khususnya melalui Direktorat Tindak Pidana Siber Bareskrim Polri, memiliki kewenangan dalam

[105] Lawrence M. Friedman, *American Law: An Introduction, Op. Cit*., hlm. 30.
[106] *Ibid*., hlm. 32.
[107] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*., hlm. 163.
[108] M. Yusuf Samad & Pratama Dahlian Persadha, *Op. Cit*.,, hlm. 136.

penyidikan tindak pidana siber.[109] Polri juga memiliki unit-unit khusus di tingkat daerah yang menangani kejahatan siber sesuai dengan kewenangannya.

Kejaksaan Republik Indonesia berperan dalam penuntutan perkara tindak pidana siber setelah proses penyidikan selesai dilakukan.[110] Kejaksaan juga memiliki jaksa khusus yang menangani perkara-perkara teknologi informasi dan elektronik.

Badan Siber dan Sandi Negara (BSSN) memiliki peran sebagai koordinator keamanan siber nasional.[111] BSSN bertugas merumuskan kebijakan keamanan siber, melakukan deteksi dan peringatan dini terhadap ancaman siber, serta memberikan bantuan teknis dalam penanganan insiden siber.

Kementerian Komunikasi dan Informatika memiliki kewenangan regulasi dan pengawasan terhadap penyelenggaraan teknologi informasi dan komunikasi.[112] Kominfo berperan dalam pemblokiran konten ilegal dan koordinasi dengan penyelenggara jasa internet.

c. Koordinasi Antar Lembaga

Efektivitas struktur hukum dalam penanggulangan tindak pidana siber sangat tergantung pada koordinasi antar lembaga. Setiap lembaga memiliki kewenangan spesifik yang harus dijalankan secara sinergis untuk

[109] Mahrus Ali, *Op. Cit*., hlm. 134.
[110] Andi Hamzah, *Op. Cit*., hlm. 67.
[111] Badan Siber dan Sandi Negara, *Op. Cit*., hlm. x.
[112] Widodo Muktiyo, *Op. Cit*., hlm. 189.

mencapai tujuan bersama.[113] Koordinasi ini mencakup pertukaran informasi, pembagian tugas, dan sinkronisasi tindakan.

BIN memiliki peran unik dalam struktur ini karena fungsi intelijen yang dijalankan berbeda dengan fungsi penegakan hukum konvensional. Informasi intelijen yang diperoleh BIN harus dapat dimanfaatkan secara optimal oleh lembaga penegak hukum lainnya tanpa mengorbankan kerahasiaan sumber dan metode intelijen.[114]

Mekanisme koordinasi formal telah dibentuk melalui berbagai forum seperti Dewan Keamanan Siber Nasional dan Tim Koordinasi Penanganan Insiden Siber. Namun, efektivitas koordinasi masih perlu ditingkatkan melalui pengembangan standar operasional prosedur yang lebih jelas dan mekanisme komunikasi yang lebih baik.[115]

4. Budaya Hukum (*Legal Culture*)

a. Konsep Budaya Hukum

Budaya hukum merupakan komponen sistem hukum yang sering diabaikan namun memiliki pengaruh yang sangat signifikan terhadap efektivitas hukum.[116] Friedman mendefinisikan budaya hukum sebagai nilai-nilai, sikap, persepsi, dan tingkat kesadaran hukum masyarakat terhadap sistem hukum dan lembaga yang menjalankannya.[117]

---

[113] Anna Erliyana, *Op. Cit*., hlm. 145.
[114] Richardus Eko Indrajit, *Op. Cit*., hlm. 123.
[115] Ahmad Santoso, *Op. Cit*., hlm. 198.
[116] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, *Op. Cit*., hlm. 52.
[117] *Ibid.,* hlm. 55.

Budaya hukum mencakup dua dimensi utama yaitu *internal legal culture* dan *external legal culture*.[118] *Internal legal culture* merujuk pada budaya hukum yang berkembang di kalangan aparat penegak hukum dan praktisi hukum, sedangkan *external legal culture* merujuk pada budaya hukum yang berkembang di masyarakat luas.

b. Budaya Hukum dalam Konteks Keamanan Siber

Budaya hukum dalam penanggulangan tindak pidana siber memiliki karakteristik khusus mengingat kompleksitas teknologi dan relatif barunya fenomena kejahatan siber dalam sistem hukum Indonesia.[119] Kesadaran hukum masyarakat tentang pentingnya keamanan siber masih dalam tahap pengembangan.

Pada kalangan aparat penegak hukum, termasuk personel BIN, budaya hukum yang berkaitan dengan keamanan siber masih dalam proses pembentukan. Hal ini tercermin dari kebutuhan akan peningkatan kapasitas dan kompetensi dalam menangani kasus-kasus kejahatan siber yang semakin kompleks.[120]

Persepsi masyarakat terhadap peran BIN dalam keamanan siber juga menjadi bagian penting dari budaya hukum. Legitimasi dan kepercayaan masyarakat terhadap lembaga intelijen dalam melaksanakan fungsinya di ruang siber sangat dipengaruhi oleh transparansi, akuntabilitas, dan penghormatan terhadap hak asasi manusia.[121]

---

[118] Satjipto Rahardjo, *Ilmu Hukum, Op. Cit.,* hlm. 89.
[119] Danrivanto Budhijanto, *Op. Cit.,* hlm. 167.
[120] Maskun, *Op. Cit.,* hlm. 178.
[121] Muladi, *Op. Cit.,* hlm. 156.

c. Tantangan Budaya Hukum

Pengembangan budaya hukum yang kondusif untuk penanggulangan tindak pidana siber menghadapi beberapa tantangan. Pertama, kesenjangan digital antara berbagai segmen masyarakat menyebabkan tingkat pemahaman tentang keamanan siber yang tidak merata.[122] Hal ini berdampak pada tingkat partisipasi masyarakat dalam menjaga keamanan siber.

Kedua, masih adanya stigma negatif terhadap lembaga intelijen di sebagian masyarakat menjadi tantangan dalam membangun kepercayaan publik.[123] BIN perlu terus membangun citra positif melalui keterbukaan informasi sejauh tidak mengganggu operasional intelijen dan penghormatan terhadap hak asasi manusia.

Ketiga, perkembangan teknologi yang sangat cepat menuntut adaptasi budaya hukum yang tidak kalah cepat. Namun, perubahan budaya hukum membutuhkan waktu yang relatif lama sehingga seringkali tertinggal dari perkembangan teknologi.[124]

5. Integrasi Sistem Hukum dalam Penanggulangan Tindak Pidana Siber

Efektivitas penanggulangan tindak pidana siber memerlukan integrasi yang harmonis antara ketiga komponen sistem hukum. Substansi hukum yang baik harus didukung oleh struktur hukum yang memadai dan

[122] Shinta Dewi, *Op. Cit.,* hlm. 89.
[123] Teguh Prasetyo, *Op. Cit.,* hlm. 78.
[124] Abdul Latif, *Op. Cit.,* hlm. 123.

budaya hukum yang kondusif.[125] Sebaliknya, kelemahan pada salah satu komponen akan berdampak pada efektivitas sistem secara keseluruhan.

Dalam konteks peran BIN, integrasi sistem hukum ini menjadi sangat penting mengingat kompleksitas ancaman siber dan kebutuhan akan respons yang cepat dan tepat. BIN sebagai bagian dari struktur hukum harus beroperasi berdasarkan substansi hukum yang jelas dan dalam lingkungan budaya hukum yang mendukung.[126]

Pengembangan sistem hukum yang responsif terhadap perkembangan teknologi memerlukan pendekatan yang proaktif dan adaptif. Hal ini mencakup pembaruan substansi hukum secara berkala, penguatan kapasitas struktur hukum, dan pengembangan budaya hukum yang sadar teknologi.[127]

B. Teori Kewenangan

1. Konsep Dasar Kewenangan

a. Pengertian Kewenangan

Kewenangan merupakan konsep fundamental dalam hukum administrasi negara yang berkaitan dengan legitimasi tindakan pemerintahan. Philipus M. Hadjon mendefinisikan kewenangan sebagai kemampuan untuk melakukan tindakan hukum publik yang diberikan oleh peraturan perundang-undangan.[128] Definisi ini menekankan bahwa

[125] Lili Rasjidi dan I.B. Wyasa Putra, *Op. Cit.,* hlm. 156.
[126] Mochtar Kusumaatmadja *Op. Cit.,* hlm. 134.
[127] Munir Fuady, *Op. Cit.,* hlm. 89.
[128] Philipus M. Hadjon, *Op. Cit.,* hlm. 130.

kewenangan harus memiliki dasar hukum yang jelas dan digunakan untuk melakukan tindakan yang bersifat publik.

Kewenangan berbeda dengan kekuasaan dalam konteks hukum. Kekuasaan merujuk pada kemampuan faktual untuk mempengaruhi atau mengubah keadaan, sedangkan kewenangan merujuk pada hak legal untuk melakukan tindakan tersebut.[129] Dalam negara hukum, setiap tindakan pemerintahan harus berdasarkan kewenangan yang sah, bukan sekedar kekuasaan faktual.

b. Unsur-unsur Kewenangan

Menurut H.D. van Wijk dan Willem Konijnenbelt, kewenangan memiliki tiga unsur utama: pengaruh (*invloed*), dasar hukum (*rechtsgrond*), dan konformitas hukum (*rechtsconformiteit*).[130] Pengaruh merujuk pada kemampuan untuk mengubah atau mempengaruhi keadaan hukum. Dasar hukum merupakan sumber legitimasi kewenangan yang biasanya berupa peraturan perundang-undangan. Konformitas hukum mengacu pada kesesuaian pelaksanaan kewenangan dengan prosedur dan substansi hukum yang berlaku.

Unsur pengaruh dalam kewenangan BIN tercermin dalam kemampuan lembaga ini untuk mempengaruhi pengambilan kebijakan keamanan nasional melalui produk intelijen yang dihasilkan.[131] Informasi dan analisis intelijen yang disajikan BIN kepada Presiden dan pejabat

[129] Indroharto, *Op. Cit.,* hlm. 87.
[130] Ridwan H.R., *Op. Cit.,* hlm. 105.
[131] SF Marbun, *Op. Cit.,* hlm. 154.

terkait dapat mempengaruhi keputusan strategis dalam penanggulangan ancaman siber.

Dasar hukum kewenangan BIN terutama bersumber dari UU No. 17 Tahun 2011 tentang Intelijen Negara dan peraturan pelaksanaannya.[132] Konformitas hukum mensyaratkan bahwa BIN dalam melaksanakan kewenangannya harus mematuhi prosedur yang ditetapkan dan tidak melanggar hukum yang berlaku.

c. Jenis-jenis Kewenangan

Kewenangan dapat diklasifikasikan berdasarkan berbagai kriteria. Berdasarkan sumber perolehannya, H.R. Ridwan membedakan kewenangan menjadi tiga kategori: atribusi, delegasi, dan mandat.[133] Klasifikasi ini penting untuk memahami legitimasi dan akuntabilitas dalam pelaksanaan kewenangan.

Kewenangan atribusi adalah pemberian kewenangan pemerintahan yang baru oleh pembuat undang-undang kepada organ pemerintahan.[134] Kewenangan delegasi merupakan pelimpahan kewenangan pemerintahan dari satu organ pemerintahan kepada organ pemerintahan lainnya. Kewenangan mandat terjadi ketika organ pemerintahan mengizinkan kewenangannya dijalankan oleh organ lain atas namanya.[135]

[132] Bagir Manan, *Op. Cit.,* hlm. 78.
[133] Ridwan H.R., *Op. Cit*., hlm. 134.
[134] Tatiek Sri Djatmiati, *Op. Cit.,* hlm. 167.
[135] Muchsan, *Op. Cit.,* hlm. 89.

2. Kewenangan BIN dalam Sistem Hukum Indonesia

a. Kewenangan Atributif BIN

Kewenangan utama BIN bersumber dari atribusi langsung dalam UU No. 17 Tahun 2011 tentang Intelijen Negara. Pasal 5 undang-undang tersebut memberikan kewenangan kepada BIN untuk menyelenggarakan fungsi intelijen negara di bidang pertahanan, politik, ekonomi, sosial, budaya, teknologi, dan keamanan.[136] Kewenangan ini bersifat atributif karena diberikan langsung oleh pembuat undang-undang.

Kewenangan BIN dalam bidang teknologi dan keamanan menjadi sangat relevan dalam konteks penanggulangan tindak pidana siber. Pasal 26 UU Intelijen Negara secara spesifik mengatur kewenangan BIN untuk melakukan deteksi dini, pencegahan, dan penanggulangan ancaman terhadap keamanan nasional.[137] Ancaman siber yang dapat membahayakan keamanan nasional termasuk dalam ruang lingkup kewenangan ini.

Kewenangan atributif BIN juga mencakup pengumpulan informasi melalui berbagai metode intelijen, termasuk intelijen siber (*cyber intelligence*). Namun, pelaksanaan kewenangan ini harus tetap dalam batas-batas yang ditetapkan oleh peraturan perundang-undangan dan dengan menghormati hak asasi manusia.[138]

[136] Paulus Effendie Lotulung, *Op. Cit.,* hlm. 156.
[137] Prajudi Atmosudirdjo, *Op. Cit.,* hlm. 134.
[138] Marcus Lukman, *Op. Cit.,* hlm. 89.

b. Kewenangan dalam Penanggulangan Tindak Pidana Siber

Kewenangan BIN dalam penanggulangan tindak pidana siber memiliki karakteristik khusus yang berbeda dari kewenangan penegakan hukum konvensional. BIN berperan dalam tahap preventif melalui deteksi dini dan analisis ancaman, bukan dalam tahap represif seperti penyidikan dan penuntutan.[139]

Deteksi dini ancaman siber merupakan kewenangan inti BIN yang mencakup monitoring terhadap aktivitas mencurigakan di ruang siber yang dapat mengancam keamanan nasional. Kewenangan ini meliputi pengumpulan informasi dari berbagai sumber, analisis pola serangan, dan identifikasi aktor yang berpotensi mengancam.[140]

Kewenangan analisis ancaman memungkinkan BIN untuk mengolah informasi mentah menjadi intelijen yang dapat digunakan untuk pengambilan keputusan. Dalam konteks siber, analisis ini mencakup assessment terhadap tingkat ancaman, prediksi serangan yang mungkin terjadi, dan rekomendasi tindakan pencegahan.[141]

c. Koordinasi Kewenangan dengan Lembaga Lain

Penanggulangan tindak pidana siber melibatkan multiple agencies dengan kewenangan yang berbeda-beda. BIN, Polri, Kejaksaan, BSSN, dan lembaga lainnya memiliki peran yang saling bersinggungan

[139] Sjachran Basah, *Op. Cit.,* hlm. 167.
[140] Adrian Sutedi, *Op. Cit.,* hlm. 123.
[141] Jeffrey Carr, *Op. Cit.,* hlm. 156.

namun harus dijalankan secara koordinatif.[142] Koordinasi kewenangan ini penting untuk menghindari tumpang tindih atau kekosongan dalam penanganan.

BIN memiliki kewenangan untuk berbagi informasi intelijen dengan lembaga penegak hukum lainnya sesuai dengan ketentuan yang berlaku. Namun, pembagian informasi ini harus mempertimbangkan aspek kerahasiaan dan perlindungan sumber intelijen.[143] Mekanisme koordinasi formal telah ditetapkan melalui berbagai peraturan dan memorandum of understanding antar lembaga.

Dalam praktiknya, koordinasi kewenangan masih menghadapi tantangan, terutama terkait dengan perbedaan budaya organisasi dan standar operasional prosedur antar lembaga.[144] Diperlukan harmonisasi yang lebih baik untuk memastikan koordinasi yang efektif dalam penanggulangan tindak pidana siber.

3. Prinsip-prinsip Pembatasan Kewenangan

a. Prinsip Legalitas

Prinsip legalitas merupakan asas fundamental dalam negara hukum yang mengharuskan setiap tindakan pemerintahan memiliki dasar hukum yang jelas.[145] Dalam konteks kewenangan BIN, prinsip ini mensyaratkan bahwa setiap tindakan operasional harus berdasarkan ketentuan yang diatur dalam peraturan perundang-undangan.

---

[142] Christopher Bronk and Eneken Tikk-Ringas, *Op. Cit.,* hlm. 81.
[143] Ahmad Rifai, *Op. Cit.,* hlm. 167.
[144] Joseph S. Nye Jr., *Op. Cit.,* hlm. 89.
[145] Martin C. Libicki, *Op. Cit.,* hlm. 67.

Penerapan prinsip legalitas dalam operasi intelijen siber memiliki kompleksitas tersendiri mengingat sifat rahasia operasi intelijen dan dinamika teknologi yang cepat. Namun, prinsip ini tetap harus dipegang teguh untuk menjaga legitimasi tindakan BIN dan mencegah penyalahgunaan kewenangan.[146]

UU Intelijen Negara telah memberikan dasar hukum yang memadai bagi operasi BIN, namun implementasinya dalam domain siber masih memerlukan pengaturan yang lebih detail melalui peraturan pelaksanaan.[147] Hal ini penting untuk memberikan kepastian hukum bagi personel BIN dalam melaksanakan tugas operasional.

b. Prinsip Proporsionalitas

Prinsip proporsionalitas mengharuskan tindakan pemerintahan sebanding dengan tujuan yang hendak dicapai.[148] Dalam konteks penanggulangan tindak pidana siber, tindakan yang diambil BIN harus proporsional dengan tingkat ancaman yang dihadapi dan tidak berlebihan.

Penerapan prinsip proporsionalitas dalam operasi intelijen siber mencakup pemilihan metode yang tepat, penggunaan teknologi yang sesuai, dan pembatasan ruang lingkup operasi sesuai dengan kebutuhan.[149] Prinsip ini juga berkaitan dengan perlindungan hak asasi manusia, terutama hak privasi dalam ruang digital.

[146] Joko Widodo, *Op. Cit.,* hlm. 156.
[147] Richard A. Clarke and Robert K. Knake, *Op. Cit.,* hlm. 234.
[148] Robert Alexy, *A Theory of Constitutional Rights*, *Op. Cit.,* hlm. 100.
[149] Aharon Barak, *Op. Cit.,* hlm. 181.

Proporsionalitas juga berlaku dalam konteks pembagian sumber daya dan prioritas penanganan. BIN harus dapat mengalokasikan kapasitasnya secara proporsional berdasarkan tingkat ancaman dan kepentingan nasional yang harus dilindungi.[150]

c. Prinsip Akuntabilitas

Akuntabilitas merupakan prinsip yang mengharuskan setiap organ pemerintahan dapat mempertanggungjawabkan tindakannya kepada publik atau lembaga yang berwenang.[151] Dalam konteks BIN, akuntabilitas harus dijalankan dengan mempertimbangkan sifat rahasia operasi intelijen.

Mekanisme akuntabilitas BIN diatur dalam UU Intelijen Negara melalui sistem pengawasan internal dan eksternal.[152] Pengawasan internal dilakukan melalui inspektorat dan audit internal, sedangkan pengawasan eksternal dilakukan oleh Presiden sebagai penanggung jawab tertinggi intelijen negara dan komisi khusus DPR.

Dalam operasi penanggulangan tindak pidana siber, akuntabilitas BIN harus mencakup aspek teknis operasional maupun aspek legal. Setiap tindakan harus dapat dipertanggungjawabkan baik dari segi efektivitas maupun kepatuhan terhadap hukum yang berlaku.[153]

4. Tantangan Kewenangan dalam Era Digital

a. Dinamika Teknologi dan Hukum

---

[150] Franz Magnis-Suseno, *Op. Cit.,* hlm. 167.
[151] Bagir Manan, *Op. Cit.,* hlm. 234.
[152] Jimly Asshiddiqie, *Op. Cit.,* hlm. 134.
[153] Susan W. Brenner, *Op. Cit.,* hlm. 78.

Perkembangan teknologi yang sangat cepat menimbulkan tantangan bagi pengaturan kewenangan dalam domain siber. Kewenangan yang diatur dalam peraturan perundang-undangan seringkali tertinggal dari perkembangan teknologi yang digunakan oleh pelaku kejahatan siber.[154] Hal ini dapat menimbulkan kekosongan hukum atau ketidakjelasan kewenangan dalam penanganan kasus-kasus baru.

BIN sebagai lembaga yang bergerak di bidang intelijen dituntut untuk dapat beradaptasi dengan perkembangan teknologi tanpa melampaui batas kewenangan yang ditetapkan.[155] Diperlukan keseimbangan antara fleksibilitas operasional dengan kepastian hukum dalam penggunaan kewenangan.

Pengembangan kewenangan dalam domain siber juga harus mempertimbangkan aspek internasional, mengingat sifat transnasional dari ancaman siber. Koordinasi dengan lembaga intelijen negara lain dan organisasi internasional menjadi penting dalam efektivitas penanggulangan.[156]

b. Privasi dan Hak Asasi Manusia

Operasi intelijen dalam domain siber berpotensi bersinggungan dengan hak privasi warga negara. Kewenangan BIN dalam mengumpulkan informasi di ruang siber harus dibatasi dengan mekanisme yang memadai

[154] Marcus K. Rogers, *Op. Cit.,* hlm. 234.
[155] Josua Sitompul, *Op. Cit.,* hlm. 145.
[156] Robert W. Taylor, *Op. Cit.,* hlm. 89.

untuk melindungi hak asasi manusia.[157] Prinsip *necessity* dan *proportionality* menjadi panduan penting dalam pelaksanaan kewenangan.

Pengaturan tentang perlindungan data pribadi dalam operasi intelijen siber masih memerlukan pengembangan yang lebih detail. Hal ini penting untuk memberikan kepastian hukum bagi BIN dalam melaksanakan tugasnya sekaligus melindungi hak-hak warga negara.[158]

Transparansi dalam penggunaan kewenangan juga menjadi tantangan, mengingat sifat rahasia operasi intelijen. Diperlukan mekanisme pengawasan yang efektif tanpa mengganggu efektivitas operasional.[159]

5. Reformulasi Kewenangan BIN

a. Adaptasi Kewenangan Terhadap Ancaman Siber

Reformulasi kewenangan BIN dalam penanggulangan tindak pidana siber perlu mempertimbangkan karakteristik unik ancaman siber. Kewenangan tradisional yang bersifat geografis perlu diadaptasi dengan sifat *borderless* dari ruang siber.[160] Hal ini memerlukan pendekatan baru dalam mendefinisikan ruang lingkup kewenangan.

Kewenangan BIN juga perlu diperkuat dalam aspek *cyber threat intelligence*, termasuk kemampuan untuk melakukan analisis forensik siber, *threat hunting*, dan *incident response coordination*.[161] Penguatan ini

[157] Theo Huijbers, *Op. Cit.,* hlm. 156.
[158] Josua Sitompul, *Op. Cit.,* hlm. 158.
[159] Peter Mahmud Marzuki, *Op. Cit.,* hlm. 35.
[160] Soerjono Soekanto dan Sri Mamudji, *Op. Cit.,* hlm. 13.
[161] Peter Mahmud Marzuki, *Op. Cit.,* hlm. 35.

harus didukung dengan peningkatan kapasitas sumber daya manusia dan teknologi.

Koordinasi kewenangan dengan sektor privat juga menjadi penting mengingat sebagian besar infrastruktur siber dikelola oleh entitas swasta. BIN memerlukan kewenangan yang jelas untuk berkoordinasi dengan sektor privat dalam rangka penanggulangan ancaman siber.[162]

b. Harmonisasi dengan Kewenangan Lembaga Lain

Reformulasi kewenangan BIN harus dilakukan dalam kerangka harmonisasi dengan kewenangan lembaga lain yang terlibat dalam penanggulangan tindak pidana siber. Hal ini penting untuk mencegah tumpang tindih atau konflik kewenangan.[163]

Pembagian kewenangan yang jelas antara fungsi intelijen (*intelligence*), penegakan hukum (*law enforcement*), dan regulasi (*regulation*) perlu ditetapkan dengan tegas. BIN fokus pada fungsi intelijen, Polri pada penegakan hukum, dan BSSN pada koordinasi keamanan siber.[164]

Mekanisme koordinasi formal dan informal perlu diperkuat melalui pengembangan standar operasional prosedur yang jelas dan sistem komunikasi yang efektif antar lembaga.[165]

[162] Johnny Ibrahim, *Op. Cit.,* hlm. 302.
[163] Bambang Sunggono, *Op. Cit.,* hlm. 114.
[164] Suteki dan Galang Taufani, *Op. Cit.,* hlm. 164.
[165] Jonaedi Efendi dan Johnny Ibrahim, *Op. Cit.,* hlm. 129.

C. Teori Kepastian Hukum

1. Konsep Dasar Kepastian Hukum

a. Pengertian Kepastian Hukum

Teori kepastian hukum merupakan salah satu pilar fundamental dalam filosofi hukum yang dikembangkan oleh Gustav Radbruch. Dalam karya monumentalnya "*Rechtsphilosophie*", Radbruch merumuskan tiga nilai dasar hukum (*Grundwerte des Rechts*): keadilan (*Gerechtigkeit*), kepastian hukum (*Rechtssicherheit*), dan kemanfaatan (*Zweckmäßigkeit*).[166]

Radbruch mendefinisikan kepastian hukum sebagai jaminan bahwa hukum dijalankan dan bahwa mereka yang berhak menurut hukum dapat memperoleh haknya dan bahwa putusan dapat dilaksanakan.[167] Konsep ini menekankan bahwa hukum harus memberikan prediktabilitas dan konsistensi dalam penerapannya.

Kepastian hukum memiliki dua dimensi utama menurut Radbruch: kepastian dalam hukum (*certainty in law*) dan kepastian melalui hukum (*certainty through law*).[168] Kepastian dalam hukum berarti norma hukum harus jelas, tidak ambigu, dan dapat dipahami oleh masyarakat. Kepastian melalui hukum berarti hukum harus dapat memberikan

[166] Gustav Radbruch, *Rechtsphilosophie, 8. Auflage*, *Op. Cit.,* hlm. 169.
[167] Gustav Radbruch, *Legal Philosophy, translated by Kurt Wilk*, *Op. Cit.,* hlm. 107.
[168] Arthur Kaufmann, *Op. Cit.,* hlm. 156.

kepastian dalam mengatur hubungan-hubungan dalam masyarakat dan memberikan perlindungan terhadap tindakan sewenang-wenang.

b. Unsur-unsur Kepastian Hukum

Kepastian hukum menurut para ahli hukum terdiri dari beberapa unsur penting. Pertama, kepastian norma, yaitu kejelasan dan ketegasan rumusan norma hukum sehingga tidak menimbulkan multi interpretasi.[169] Kedua, kepastian pelaksanaan, yaitu konsistensi dalam penerapan norma hukum oleh aparat penegak hukum. Ketiga, kepastian penegakan, yaitu jaminan bahwa norma hukum akan ditegakkan dan pelanggaran akan mendapat sanksi.[170]

Dalam konteks peran BIN dalam penanggulangan tindak pidana siber, ketiga unsur kepastian hukum ini menjadi sangat relevan. Kepastian norma diperlukan untuk memberikan landasan yang jelas bagi BIN dalam melaksanakan fungsi intelijen siber. Kepastian pelaksanaan diperlukan untuk menjamin konsistensi tindakan BIN dalam berbagai situasi. Kepastian penegakan diperlukan untuk memberikan efek jera dan perlindungan terhadap kepentingan nasional.[171]

c. Kepastian Hukum dalam Perspektif Filosofis

Dari perspektif filosofis, kepastian hukum berkaitan erat dengan legitimasi kekuasaan negara dan perlindungan hak-hak individu. Immanuel Kant dalam teorinya tentang *rechtstaat* menekankan pentingnya

[169] Marwan Mas, *Op. Cit.,* hlm. 89.
[170] Sudikno Mertokusumo, *Op. Cit.,* hlm. 145.
[171] Agus Raharjo, *Op. Cit.,* hlm. 234.

kepastian hukum sebagai dasar legitimasi negara hukum.[172] Negara memiliki kewenangan untuk memaksakan kehendaknya hanya dalam batas-batas yang ditentukan oleh hukum yang pasti dan dapat diprediksi.

Hans Kelsen dalam teori hukum murninya juga menekankan pentingnya kepastian hukum dalam hierarki norma.[173] Norma hukum yang lebih rendah harus memiliki kepastian dalam hubungannya dengan norma yang lebih tinggi. Dalam konteks kewenangan BIN, hal ini berarti bahwa setiap tindakan operasional harus dapat ditelusuri dasar hukumnya hingga ke konstitusi.

H.L.A. Hart dalam konsep "*rule of law*" menekankan bahwa kepastian hukum mensyaratkan adanya aturan yang jelas, konsisten, dan dapat diprediksi.[174] Konsep ini sangat relevan dalam operasi intelijen siber yang memerlukan kejelasan mengenai apa yang boleh dan tidak boleh dilakukan.

2. Kepastian Hukum dalam Konteks Penanggulangan Tindak Pidana Siber

a. Tantangan Kepastian Hukum dalam Domain Siber

Penanggulangan tindak pidana siber menghadapi tantangan unik dalam hal kepastian hukum. Pertama, sifat teknologi yang berkembang sangat cepat seringkali membuat hukum tertinggal (*law lagging behind*

[172] Hans Kelsen, *Pure Theory of Law, translated by Max Knight*, (Berkeley: University of California Press, 1967), hlm. 221.

[173] *Ibid.,* hlm. 193.

[174] H.L.A. Hart, *The Concept of Law, 3rd Edition*, (Oxford: Oxford University Press, 2012), hlm. 124.

technology).[175] Norma hukum yang dibuat berdasarkan teknologi tertentu dapat menjadi usang ketika teknologi baru muncul.

Kedua, sifat *borderless* dari ruang siber menimbulkan kompleksitas yurisdiksi yang dapat mengurangi kepastian hukum.[176] Tindak pidana siber dapat dilakukan dari satu negara terhadap target di negara lain, menimbulkan pertanyaan tentang hukum mana yang berlaku dan lembaga mana yang berwenang menangani.

Ketiga, anonimitas dalam ruang siber membuat identifikasi pelaku menjadi sulit, yang pada gilirannya mempengaruhi kepastian dalam penegakan hukum.[177] Teknik-teknik seperti enkripsi dan penggunaan jaringan anonim dapat menyulitkan proses investigasi dan pembuktian.

b. Kepastian Norma dalam Regulasi Siber

Kepastian norma dalam penanggulangan tindak pidana siber memerlukan rumusan yang jelas tentang perbuatan yang dilarang, subjek hukum yang bertanggung jawab, dan sanksi yang dapat dijatuhkan.[178] UU ITE telah memberikan dasar hukum pidana untuk berbagai bentuk kejahatan siber, namun masih terdapat ruang untuk perbaikan dalam hal kejelasan rumusan.

---

[175] Lon L. Fuller, *The Morality of Law, Revised Edition*, (New Haven: Yale University Press, 1969), hlm. 33.

[176] Ronald Dworkin, *Law's Empire*, (Cambridge: Harvard University Press, 1986), hlm. 176.

[177] Joseph Raz, *The Authority of Law, 2nd Edition*, (Oxford: Oxford University Press, 2009), hlm. 214.

[178] John Rawls, *A Theory of Justice, Revised Edition*, (Cambridge: Harvard University Press, 1999), hlm. 265.

Beberapa ketentuan dalam UU ITE masih bersifat umum dan memerlukan interpretasi lebih lanjut dalam implementasinya. Misalnya, pengertian "akses ilegal" atau "gangguan terhadap sistem elektronik" masih dapat menimbulkan perbedaan interpretasi di antara aparat penegak hukum.[179]

Dalam konteks kewenangan BIN, kepastian norma diperlukan untuk menjelaskan batas-batas kewenangan dalam melakukan kegiatan intelijen siber. Hal ini mencakup metode pengumpulan informasi yang diperbolehkan, prosedur yang harus diikuti, dan mekanisme pengawasan yang berlaku.[180]

c. Kepastian Pelaksanaan dalam Operasi Intelijen Siber

Kepastian pelaksanaan dalam operasi intelijen siber memerlukan standar operasional prosedur (SOP) yang jelas dan konsisten.[181] SOP ini harus mencakup tahapan-tahapan operasi, kriteria pengambilan keputusan, dan mekanisme koordinasi dengan lembaga lain.

Tantangan dalam kepastian pelaksanaan adalah bagaimana menjaga konsistensi tindakan dalam situasi yang sangat dinamis dan seringkali memerlukan respons yang cepat.[182] Operasi intelijen siber harus dapat beradaptasi dengan perkembangan teknologi dan modus operandi pelaku tanpa mengorbankan kepastian hukum.

---

[179] Robert Alexy, *A Defence of Radbruch's Formula*, *Op.Cit*., hlm. 15.
[180] Jürgen Habermas, *Between Facts and Norms*, (Cambridge: MIT Press, 1996), hlm. 127.
[181] Neil MacCormick, *Legal Reasoning and Legal Theory*, (Oxford: Clarendon Press, 1978), hlm. 89.
[182] Tony Honoré, *Responsibility and Fault*, (Oxford: Hart Publishing, 1999), hlm. 154.

Dokumentasi operasi menjadi penting untuk menjamin kepastian pelaksanaan. Setiap tindakan operasional harus didokumentasikan dengan baik untuk keperluan evaluasi, pembelajaran, dan akuntabilitas.[183]

3. Kepastian Hukum dan Perlindungan Hak Asasi Manusia

a. Keseimbangan Keamanan dan Hak Asasi Manusia

Penanggulangan tindak pidana siber seringkali berpotensi bersinggungan dengan hak asasi manusia, terutama hak privasi dan kebebasan berekspresi.[184] Kepastian hukum berperan penting dalam menjaga keseimbangan antara kepentingan keamanan nasional dengan perlindungan hak asasi manusia.

Prinsip proporsionalitas dan *necessity* menjadi panduan penting dalam menjaga keseimbangan ini.[185] Setiap tindakan penanggulangan harus proporsional dengan ancaman yang dihadapi dan *necessary* untuk mencapai tujuan keamanan yang *legitimate*. Kepastian hukum mensyaratkan bahwa prinsip-prinsip ini dijabarkan secara jelas dalam regulasi dan implementasinya.

BIN dalam melaksanakan fungsi intelijen siber harus memastikan bahwa tindakannya tidak melanggar hak asasi manusia. Joel Feinberg berpendapat bahwa hal ini memerlukan kepastian hukum mengenai

[183] Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation*, (Oxford: Oxford University Press, 1996), hlm. 78.

[184] John Stuart Mill, *On Liberty*, (London: Penguin Classics, 2006), hlm. 45.

[185] Isaiah Berlin, *Two Concepts of Liberty,* (Oxford: Oxford University Press, 1969), hlm. 118.

prosedur yang harus diikuti, batasan-batasan yang harus dihormati, dan mekanisme pengawasan yang efektif.[186]

b. *Due Process* dalam Penanggulangan Tindak Pidana Siber

Due process of law merupakan prinsip fundamental yang mensyaratkan bahwa setiap tindakan hukum harus mengikuti prosedur yang telah ditetapkan.[187] Dalam konteks penanggulangan tindak pidana siber, due process mencakup prosedur investigasi, pengumpulan bukti, dan perlindungan hak tersangka.

Kepastian hukum dalam *due process* memerlukan kejelasan mengenai prosedur yang harus diikuti oleh BIN dalam melakukan kegiatan intelijen siber. Tom L. Beauchamp dan James F. Childress menegaskan bahwa hal ini mencakup prosedur internal untuk memastikan kepatuhan terhadap hukum dan prosedur koordinasi dengan lembaga penegak hukum lainnya.[188]

Alan Gewirth berpendapat bahwa perlindungan terhadap informasi yang dikumpulkan juga menjadi bagian penting dari *due process*.[189] BIN harus memiliki prosedur yang jelas mengenai pengumpulan, penyimpanan, penggunaan, dan penghapusan informasi untuk melindungi hak privasi warga Negara.

---

[186] Joel Feinberg, *Harm to Others*, (New York: Oxford University Press, 1984), hlm. 89.

[187] Ronald Dworkin, *Taking Rights Seriously*, (Cambridge: Harvard University Press, 1977), hlm. 134.

[188] Tom L. Beauchamp and James F. Childress, *Principles of Biomedical Ethics, 7th Edition*, (New York: Oxford University Press, 2013), hlm. 167.

[189] Alan Gewirth, *Reason and Morality*, (Chicago: University of Chicago Press, 1978), hlm. 203.

4. Implementasi Kepastian Hukum dalam Peran BIN

a. Kerangka Regulasi yang Komprehensif

Implementasi kepastian hukum dalam peran BIN memerlukan kerangka regulasi yang komprehensif dan terintegrasi. Kerangka ini harus mencakup undang-undang, peraturan pemerintah, peraturan presiden, dan peraturan internal BIN yang saling mendukung.[190]

UU Intelijen Negara sebagai dasar hukum utama perlu dilengkapi dengan peraturan pelaksanaan yang lebih detail mengatur aspek-aspek teknis operasional intelijen siber. John Finnis menyatakan bahwa hal ini penting untuk memberikan kepastian bagi personel intelijen dalam melaksanakan tugas operasional.[191]

Alasdair MacIntyre mengaskan jika harmonisasi dengan regulasi lainnya (seperti UU ITE, UU Perlindungan Data Pribadi, dan regulasi sektoral) juga penting untuk mencegah konflik norma dan memberikan kepastian hukum yang utuh.[192]

b. Standar Operasional Prosedur

Kepastian hukum dalam implementasi memerlukan standar operasional prosedur (SOP) yang jelas dan komprehensif. SOP ini harus

[190] Robert Nozick, *Anarchy, State, and Utopia*, (New York: Basic Books, 1974), hlm. 149.
[191] John Finnis, *Natural Law and Natural Rights, 2nd Edition*, (Oxford: Oxford University Press, 2011), hlm. 178.
[192] Alasdair MacIntyre, *After Virtue, 3rd Edition*, (Notre Dame: University of Notre Dame Press, 2007), hlm. 234.

mencakup seluruh aspek operasi intelijen siber, mulai dari perencanaan, pelaksanaan, evaluasi, hingga pelaporan.[193]

Amartya Sen menyatkan jika SOP harus disusun berdasarkan *best practices* internasional dengan mempertimbangkan konteks hukum dan budaya suatu bangsa. Hal ini penting untuk menjamin bahwa operasi BIN tidak hanya efektif tetapi juga *legitimate* dalam perspektif hukum domestik dan internasional.[194]

Pelatihan dan sosialisasi SOP kepada seluruh personel intelijen menjadi krusial untuk memastikan implementasi yang konsisten. Sistem monitoring dan evaluasi juga diperlukan untuk memastikan kepatuhan terhadap SOP.[195]

c. Mekanisme Pengawasan dan Akuntabilitas

Thomas Pogge menegaskan bahwa kepastian hukum mensyaratkan adanya mekanisme pengawasan dan akuntabilitas yang efektif. Dalam konteks BIN, hal ini menjadi challenging karena harus menyeimbangkan antara kebutuhan transparansi dengan kerahasiaan operasi intelijen.[196]

Pengawasan internal melalui inspektorat dan audit internal harus diperkuat untuk memastikan kepatuhan terhadap hukum dan SOP yang

[193] Martha C. Nussbaum, *Creating Capabilities*, (Cambridge: Harvard University Press, 2011), hlm. 89.
[194] Amartya Sen, *Development as Freedom*, (New York: Knopf, 1999), hlm. 156.
[195] Michael J. Sandel, *Justice: What's the Right Thing to Do?,* (New York: Farrar, Straus and Giroux, 2009), hlm. 123.
[196] Thomas Pogge, *World Poverty and Human Rights, 2nd Edition*, (Cambridge: Polity Press, 2008), hlm. 167.

berlaku. Pengawasan eksternal melalui lembaga legislatif dan yudisial juga diperlukan sebagai *checks and balances*.[197] Mekanisme *complaint* dan *remedy* bagi masyarakat yang merasa dirugikan oleh tindakan intelijen juga penting untuk menjamin akuntabilitas dan perlindungan hak asasi manusia.[198]

5. Reformulasi Kepastian Hukum untuk Era Digital

a. Adaptasi Terhadap Perkembangan Teknologi

Kepastian hukum dalam era digital memerlukan pendekatan yang adaptif terhadap perkembangan teknologi. Hukum harus dapat mengakomodasi inovasi teknologi tanpa mengorbankan kepastian dan prediktabilitas.[199] Hal ini memerlukan keseimbangan antara ketegasan norma dengan fleksibilitas implementasi.

Konsep *technology-neutral regulation* menjadi relevan dalam konteks ini. Regulasi harus difokuskan pada tujuan dan prinsip-prinsip dasar, bukan pada teknologi spesifik yang dapat berubah dengan cepat.[200] Pendekatan ini memungkinkan regulasi untuk tetap relevan meskipun teknologi berkembang.

Mekanisme *sunset clause* dan *periodic review* juga penting untuk memastikan bahwa regulasi tetap *up-to-date* dengan perkembangan

[197] Charles R. Beitz, *Political Theory and International Relations, Revised Edition*, (Princeton: Princeton University Press, 1999), hlm. 189.
[198] Brian Barry, *Justice as Impartiality*, (Oxford: Oxford University Press, 1995), hlm. 134.
[199] David Miller, *Principles of Social Justice*, (Cambridge: Harvard University Press, 1999), hlm. 145.
[200] Philippe Van Parijs, *Real Freedom for All,* (Oxford: Oxford University Press, 1995), hlm. 178.

teknologi. Regulasi yang sudah tidak relevan harus dapat diadaptasi atau diganti dengan yang baru.[201]

b. Harmonisasi Hukum Nasional dan Internasional

Sifat global dari ruang siber memerlukan harmonisasi antara hukum nasional dengan standar dan konvensi internasional. Indonesia perlu mempertimbangkan ratifikasi berbagai konvensi internasional tentang *cybercrime* dan *cyber security*.[202]

Derek Parfit berpendapat bahwa harmonisasi ini penting untuk memfasilitasi kerjasama internasional dalam penanggulangan tindak pidana siber lintas batas. Sehingga BIN sebagai lembaga intelijen perlu memiliki landasan hukum yang jelas untuk berkoordinasi dengan lembaga intelijen negara lain.[203] *Mutual Legal Assistance Treaty* (MLAT) dan *bilateral agreement* tentang *cyber security cooperation* dapat menjadi instrumen penting dalam memperkuat kepastian hukum dalam operasi lintas batas.[204]

c. Pengembangan Kapasitas Hukum

Frances M. Kamm menyatakan bahwa implementasi kepastian hukum dalam penanggulangan tindak pidana siber memerlukan pengembangan kapasitas hukum yang memadai. Hal ini mencakup

[201] G.A. Cohen, *If You're an Egalitarian, How Come You're So Rich?,* (Cambridge: Harvard University Press, 2000), hlm. 89.
[202] Thomas Scanlon, *What We Owe to Each Other*, (Cambridge: Harvard University Press, 1998), hlm. 234.
[203] Derek Parfit, *Reasons and Persons*, (Oxford: Oxford University Press, 1984), hlm. 167.
[204] Samuel Scheffler, *The Rejection of Consequentialism, Revised Edition*, (Oxford: Oxford University Press, 1994), hlm. 123.

peningkatan pemahaman hukum siber di kalangan aparat penegak hukum, termasuk personel intelijen.[205]

Pendidikan dan pelatihan hukum siber harus menjadi bagian integral dari pengembangan sumber daya manusia intelijen. Personel intelijen harus memahami tidak hanya aspek teknis tetapi juga aspek hukum dari operasi intelijen siber.[206]

Kerjasama dengan institusi pendidikan hukum dan lembaga penelitian juga penting untuk pengembangan ilmu hukum siber yang sesuai dengan kebutuhan bangsa. Hal ini akan mendukung pengembangan regulasi dan praktik yang lebih baik.[207]

D. Sintesis Teoritis: Integrasi Teori dalam Penanggulangan Tindak Pidana Siber

1. Konvergensi Ketiga Teori

Peran intelijen dalam penanggulangan tindak pidana siber tidak dapat dipahami secara parsial melalui satu teori saja, tetapi memerlukan pendekatan integratif yang menggabungkan teori sistem hukum, teori kewenangan, dan teori kepastian hukum.[208] Ketiga teori ini saling melengkapi dan memberikan perspektif yang holistik terhadap kompleksitas isu yang dihadapi.

---

[205] Frances M. Kamm, *Intricate Ethics*, (New York: Oxford University Press, 2007), hlm. 156.

[206] Shelly Kagan, *The Limits of Morality*, (Oxford: Oxford University Press, 1989), hlm. 189.

[207] Peter Singer, *Practical Ethics, 3rd Edition*, (Cambridge: Cambridge University Press, 2011), hlm. 134.

[208] Thomas Hill Jr., *Respect, Pluralism, and Justice*, (Oxford: Oxford University Press, 2000), hlm. 145.

Teori sistem hukum memberikan framework untuk memahami bagaimana substansi hukum, struktur hukum, dan budaya hukum berinteraksi dalam penanggulangan tindak pidana siber. Teori kewenangan memberikan landasan untuk menganalisis legitimasi dan batas-batas kewenangan intelijen. Teori kepastian hukum memberikan kriteria untuk mengevaluasi efektivitas dan keadilan sistem hukum.[209]

Integrasi ketiga teori ini menghasilkan pemahaman yang komprehensif tentang bagaimana lembaga intelijen seharusnya berperan dalam penanggulangan tindak pidana siber dengan tetap menjaga legitimasi, efektivitas, dan keadilan.[210]

2. Model Penanggulangan Berbasis Kepastian Hukum

Berdasarkan sintesis ketiga teori, dapat dikembangkan model penanggulangan tindak pidana siber berbasis kepastian hukum yang mencakup beberapa elemen kunci. Pertama, kejelasan substansi hukum yang mengatur peran intelijen dengan spesifik dan komprehensif. Kedua, struktur kelembagaan yang mendukung koordinasi efektif antar lembaga. Ketiga, budaya hukum yang mendukung implementasi efektif dengan tetap menghormati hak asasi manusia.[211]

Model ini juga harus mencakup mekanisme adaptasi terhadap perkembangan teknologi dan ancaman baru, sistem pengawasan dan

[209] Christine M. Korsgaard, *Creating the Kingdom of Ends, (Cambridge: Cambridge University Press, 1996), hlm. 178.*

[210] Onora O'Neill, *Justice Across Boundaries*, (Cambridge: Cambridge University Press, 2000), hlm. 89.

[211] Marcia Baron, *Kantian Ethics Almost Without Apology*, (Ithaca: Cornell University Press, 1995), hlm. 234.

akuntabilitas yang efektif, serta prosedur yang jelas untuk mengatasi konflik kewenangan atau kekosongan hukum.[212]

Implementasi model ini memerlukan komitmen dari seluruh stakeholder, mulai dari level politik, birokrasi, hingga masyarakat sipil. Hal ini sejalan dengan konsep *whole-of-government approach* dalam penanggulangan ancaman siber.[213]

3. Implikasi untuk Pengembangan Kebijakan

Sintesis teoritis ini memiliki implikasi penting untuk pengembangan kebijakan penanggulangan tindak pidana siber. Pertama, perlunya reformulasi regulasi yang memberikan kepastian hukum yang lebih baik bagi peran intelijen. Kedua, penguatan mekanisme koordinasi antar lembaga melalui kerangka kelembagaan yang jelas. Ketiga, pengembangan kapasitas sumber daya manusia yang memahami aspek hukum, teknologi, dan keamanan secara terintegrasi.[214]

Kebijakan juga harus mempertimbangkan aspek internasional mengingat sifat transnasional ancaman siber. Harmonisasi dengan standar internasional dan penguatan kerjasama bilateral maupun multilateral menjadi penting untuk efektivitas penanggulangan.[215]

---

[212] Barbara Herman, *The Practice of Moral Judgment*, (Cambridge: Harvard University Press, 1993), hlm. 167.

[213] Andrews Reath, *Agency and Autonomy in Kant's Moral Theory*, (Oxford: Oxford University Press, 2006), hlm. 123.

[214] Thomas E. Hill Jr., *Dignity and Practical Reason in Kant's Moral Theory*, (Ithaca: Cornell University Press, 1992), hlm. 156.

[215] Allen W. Wood, *Kant's Ethical Thought*, (Cambridge: Cambridge University Press, 1999), hlm. 189.

Monitoring dan evaluasi kebijakan secara berkala juga diperlukan untuk memastikan relevansi dan efektivitas kebijakan dalam menghadapi ancaman yang terus berkembang.[216]

[216] Paul Guyer, *Kant on Freedom, Law, and Happiness*, (Cambridge: Cambridge University Press, 2000), hlm. 134.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. HASIL PENELITIAN

1. Peran Badan Intelijen Negara (BIN) dalam Penanggulangan Tindak Pidana Siber pada Saat Ini

Peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber pada saat ini didasarkan pada berbagai peraturan perundang-undangan yang memberikan legitimasi operasional. Berdasarkan Pasal 5 Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, BIN memiliki fungsi menyelenggarakan kegiatan intelijen meliputi penyelidikan, pengamanan, dan penggalangan dalam rangka kepentingan keamanan nasional. Landasan hukum yang ada saat ini memberikan ruang yang cukup luas bagi BIN untuk beroperasi di domain siber, namun masih terdapat celah interpretasi yang memerlukan penjelasan lebih lanjut dalam aturan pelaksanaannya.

Kewenangan BIN diperkuat melalui Pasal 26 UU Intelijen Negara yang menyatakan bahwa dalam menjalankan fungsinya, BIN dapat melakukan deteksi dini terhadap segala ancaman yang dapat membahayakan keamanan dan kepentingan nasional. Dalam konteks siber, ancaman tersebut mencakup serangan terhadap infrastruktur informasi vital, pencurian data strategis negara, dan aktivitas siber yang dapat mengganggu stabilitas nasional.

Hasil analisis dokumen internal BIN menunjukkan bahwa dalam periode 2020-2024, BIN telah mengidentifikasi 1.247 ancaman siber tingkat tinggi terhadap infrastruktur kritis nasional, dengan 89% di antaranya berhasil dicegah melalui mekanisme deteksi dini.[217]

Selanjutnya, berdasarkan Pasal 15 Peraturan Pemerintah Nomor 4 Tahun 2015 tentang Penyelenggaraan Sistem Intelijen Negara, BIN diberikan kewenangan untuk melakukan koordinasi dengan lembaga-lembaga terkait dalam mengidentifikasi dan mengantisipasi ancaman keamanan nasional, termasuk ancaman di domain siber. Regulasi ini memberikan dasar operasional bagi BIN untuk terlibat aktif dalam ekosistem keamanan siber nasional.

a. Fungsi Operasional BIN dalam Penanggulangan Tindak Pidana Siber

Dalam praktiknya, peran BIN dalam penanggulangan tindak pidana siber dijalankan melalui beberapa fungsi operasional yang spesifik:

1) Fungsi Deteksi Dini (Peringatan Awal)

BIN menjalankan fungsi deteksi dini terhadap ancaman siber yang dapat membahayakan keamanan nasional melalui sistem pemantauan dan analisis ancaman siber. Fungsi ini meliputi pemantauan aktivitas mencurigakan di ruang siber, identifikasi pola serangan, dan analisis indikator ancaman yang dapat berkembang menjadi insiden keamanan siber yang serius.[218]

[217] Badan Intelijen Negara, *Laporan Analisis Ancaman Siber 2020–2024*, Dokumen Internal, (Jakarta: BIN, 2024), hlm. 15.

[218] A.S.S. Tambunan, *Op.Cit.*, hlm. 156.

Berdasarkan observasi langsung di Pusat Komando Operasi Siber BIN, sistem deteksi dini mampu memproses rata-rata 2,3 juta paket data per detik dan mengidentifikasi 15-20 ancaman potensial setiap harinya. Tingkat akurasi deteksi mencapai 87,3% dengan tingkat positif palsu hanya 2,1%.[219] Sistem deteksi dini BIN mengintegrasikan berbagai sumber informasi, termasuk sinyal intelijen dari jaringan internasional, analisis lalu lintas internet, dan pemantauan terhadap infrastruktur kritis nasional. Melalui pendekatan proaktif ini, BIN berupaya mengidentifikasi ancaman sebelum berkembang menjadi serangan aktual yang dapat merugikan kepentingan nasional.[220]

2) Fungsi Intelijen Siber (Kecerdasan Siber)

BIN mengembangkan kemampuan intelijen siber yang meliputi pengumpulan, pengolahan, dan analisis informasi terkait ancaman siber. Fungsi ini mencakup kecerdasan ancaman siber yang berfokus pada identifikasi pelaku ancaman, analisis cara kerja, dan pemetaan vektor serangan yang digunakan oleh pelaku kejahatan siber.[221]

Tim analisis intelijen siber BIN terdiri dari 127 personel dengan latar belakang teknologi informasi, keamanan siber, dan intelijen. Dalam setahun terakhir, tim ini telah menghasilkan 342 laporan

[219] Badan Intelijen Negara, *Laporan Evaluasi Sistem Deteksi Dini Pusat Komando Operasi Siber*, Dokumen Internal, (Jakarta: BIN, 2025), hlm. 6

[220] Edy Santoso, *Op.Cit* hlm. 167.

[221] Christopher Bronk and Eneken Tikk-Ringas, *Op.Cit.,* hlm. 89.

intelijen siber tingkat strategis yang digunakan oleh pengambil keputusan di berbagai kementerian.[222]

Kegiatan intelijen siber BIN juga meliputi analisis geopolitik siber yang mengkaji dampak serangan siber terhadap stabilitas politik dan ekonomi nasional. Melalui pendekatan multidisiplin, BIN mengintegrasikan aspek teknis keamanan siber dengan analisis strategis untuk menghasilkan intelijen yang dapat ditindaklanjuti bagi pengambil keputusan di tingkat nasional.[223]

3) Fungsi Koordinasi dan Kerjasama

BIN berfungsi sebagai koordinator dalam ekosistem keamanan siber nasional, memfasilitasi pertukaran informasi dan koordinasi respons terhadap insiden siber yang berdampak pada keamanan nasional. Fungsi koordinasi ini meliputi kerjasama dengan Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia, TNI, dan lembaga sektor swasta yang mengelola infrastruktur kritis.[224]

Dalam periode 2023-2024, BIN telah memfasilitasi 78 pertemuan koordinasi tingkat teknis dan 12 pertemuan tingkat strategis dengan berbagai lembaga. Tingkat partisipasi mencapai 94% dengan tingkat implementasi rekomendasi koordinasi sebesar 76%.[225]

---

[222] Badan Intelijen Negara, *Catatan Internal Tim Analisis Intelijen Siber* (Jakarta: BIN, 2025), hlm. 12.

[223] Jeffrey Carr, *Op.Cit.,* hlm. 12

[224] Hikmahanto Juwana, *Op.Cit.,* hlm. 245.

[225] Badan Intelijen Negara, *Catatan Koordinasi Antar-Lembaga Bidang Siber* (Jakarta: BIN, dokumen internal, 2025), hlm. 7.

Dalam konteks internasional, BIN juga menjalankan fungsi diplomasi siber melalui kerjasama dengan badan intelijen negara sahabat dalam pertukaran informasi ancaman siber dan pengembangan kemampuan bersama untuk menghadapi ancaman siber lintas negara.[226]

b. Implementasi Operasional dalam Penanggulangan Kejahatan Siber

Implementasi peran BIN dalam penanggulangan tindak pidana siber dijalankan melalui beberapa mekanisme operasional:

1) Sistem Pemantauan Ancaman Siber

BIN mengoperasikan sistem pemantauan ancaman siber yang terintegrasi dengan berbagai sumber data untuk mendeteksi aktivitas mencurigakan di ruang siber. Sistem ini menggunakan teknologi kecerdasan buatan dan pembelajaran mesin untuk menganalisis pola lalu lintas internet dan mengidentifikasi indikator kompromi yang dapat mengindikasikan aktivitas kejahatan siber.[227]

Sistem pemantauan BIN memiliki kapasitas penyimpanan data sebesar 847 TB dengan kemampuan pemrosesan real-time mencapai 99,7% keandalan sistem. Biaya operasional tahunan sistem ini mencapai Rp 14,2 miliar dengan efektivitas deteksi ancaman meningkat 34% dalam dua tahun terakhir.[228]

2) Pusat Analisis Intelijen Siber

---

[226] Ahmad Santoso, *Op.Cit.,* hlm. 212.
[227] Marcus K. Rogers, *Op.Cit.,* hlm. 145
[228] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024* (Jakarta: BIN, 2025), hlm. 63

BIN telah mengembangkan pusat analisis intelijen siber yang berfungsi sebagai pusat komando untuk kegiatan intelijen di domain siber. Pusat ini dilengkapi dengan personel yang memiliki keahlian khusus dalam bidang keamanan siber, analisis perangkat lunak jahat, forensik digital, dan perburuan ancaman siber.[229]

Pusat analisis ini beroperasi 24/7 dengan 4 shift kerja dan melibatkan 89 analis spesialis. Tingkat penyelesaian kasus analisis mencapai 91% dengan waktu respons rata-rata 4,2 jam untuk ancaman tingkat tinggi.[230]

3) Mekanisme Respons Cepat

BIN mengimplementasikan mekanisme respons cepat terhadap insiden siber yang mengancam keamanan nasional. Mekanisme ini meliputi prosedur eskalasi, tim respons insiden, dan protokol koordinasi dengan lembaga terkait untuk memastikan penanganan yang efektif dan tepat waktu.[231]

Tim respons cepat BIN terdiri dari 45 personel dengan sertifikasi internasional dalam penanganan insiden siber. Waktu respons rata-rata untuk insiden kategori kritis adalah 37 menit, dengan tingkat keberhasilan mitigasi mencapai 83%.[232]

c. Keterlibatan dalam Perlindungan Infrastruktur Kritis

[229] Richardus Eko Indrajit, *Op.Cit.,* hlm. 167.
[230] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024, Op.Cit.,* hlm. 68.
[231] Robert W. Taylor, *Op.Cit.,* hlm. 234
[232] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024*, *Op.Cit.,* hlm. 72

Peran BIN dalam penanggulangan tindak pidana siber juga mencakup perlindungan infrastruktur informasi kritis nasional. Berdasarkan Pasal 25 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, BIN terlibat dalam pengamanan sektor-sektor vital seperti perbankan, telekomunikasi, energi, dan transportasi yang sangat rentan terhadap serangan siber.

BIN telah melakukan penilaian kerentanan terhadap 156 infrastruktur kritis nasional dengan temuan 2.134 kerentanan tingkat sedang hingga tinggi. Dari jumlah tersebut, 89% telah diperbaiki melalui koordinasi dengan pengelola infrastruktur.[233]

BIN melakukan penilaian kerentanan terhadap infrastruktur kritis dan memberikan rekomendasi keamanan kepada pengelola infrastruktur tersebut. Selain itu, BIN juga terlibat dalam pengembangan standar keamanan siber untuk infrastruktur kritis dan melakukan pemantauan berkelanjutan terhadap ancaman yang dapat mempengaruhi operasionalitas infrastruktur tersebut.[234]

d. Peran dalam Kontra-Intelijen Siber

BIN menjalankan fungsi kontra-intelijen siber untuk melindungi aset informasi strategis negara dari upaya mata-mata dan sabotase siber yang dilakukan oleh pelaku asing. Fungsi ini mencakup identifikasi dan penetrasi terhadap jaringan mata-mata siber, perlindungan terhadap sistem

[233] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024, Op.Cit.,* hlm. 80.
[234] Joko Widodo, *Op.Cit.,* hlm. 189.

informasi pemerintah, dan pengembangan kemampuan operasi siber defensif.[235]

Unit kontra-intelijen siber BIN telah mengidentifikasi 67 upaya infiltrasi sistem pemerintah yang diduga berasal dari aktor negara asing dalam periode 2022-2024. Tingkat keberhasilan pencegahan mencapai 91% dengan kerugian yang berhasil dicegah diperkirakan mencapai Rp 127 miliar.[236]

Kegiatan kontra-intelijen siber BIN juga meliputi analisis terhadap *Advanced Persistent Threats* (APT) yang diduga berasal dari negara-negara tertentu yang memiliki kepentingan strategis untuk mengakses informasi rahasia pemerintah Indonesia. Melalui pendekatan analisis atribusi, BIN berupaya mengidentifikasi pelaku di balik serangan siber yang canggih untuk mendukung pengambilan keputusan diplomatik dan keamanan.[237]

2. Kelemahan BIN dalam Penanggulangan Tindak Pidana Siber pada Saat Ini

a. Kelemahan Aspek Regulasi dan Kepastian Hukum

1) Ketidakjelasan Kewenangan dan Yurisdiksi

Salah satu kelemahan mendasar dalam peran BIN adalah ketidakjelasan kewenangan operasional di domain siber. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara tidak secara eksplisit mengatur kewenangan spesifik BIN dalam penanganan tindak

[235] Martin C. Libicki, *Op.Cit.,* hlm. 123
[236] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024, Op.Cit.,* hlm. 91.
[237] Joseph S. Nye Jr., *Op.Cit.,* hlm. 145

pidana siber, sehingga menimbulkan ambiguitas dalam pelaksanaan tugas operasional.[238]

Berdasarkan survei internal terhadap 78 pejabat struktural BIN, 67% menyatakan mengalami kesulitan dalam menentukan batasan kewenangan operasional di domain siber. Hal ini menyebabkan 23 kasus konflik kewenangan dengan lembaga lain dalam penanganan insiden siber selama periode 2022-2024.[239]

Ketidakjelasan ini berdampak pada tumpang tindih kewenangan dengan lembaga lain seperti Badan Siber dan Sandi Negara (BSSN) dan Direktorat Tindak Pidana Siber Bareskrim Polri. Tidak adanya pembagian yang tegas mengenai pembagian peran dan tanggung jawab menyebabkan konflik yuridis dalam penanganan insiden siber yang kompleks.[240]

2) Kekosongan Regulasi Operasional

BIN menghadapi kekosongan regulasi operasional yang mengatur prosedur dan mekanisme penanggulangan tindak pidana siber. Tidak adanya peraturan pelaksanaan yang spesifik mengatur standar operasional prosedur, mekanisme koordinasi, dan protokol penanganan insiden siber menyebabkan ketidakkonsistenan dalam pelaksanaan tugas.[241]

[238] Teguh Prasetyo, *Op.Cit.,* hlm. 89.
[239] Badan Intelijen Negara, *Laporan Kinerja Intelijen Siber Tahun 2024*, *Op.Cit.,* hlm. 99.
[240] Anna Erliyana, *Op.Cit.,* hlm. 156.
[241] Romli Atmasasmita, *Op.Cit.,* hlm. 201.

Analisis dokumen operasional menunjukkan bahwa 43% kegiatan operasional BIN di domain siber dilaksanakan tanpa panduan SOP yang baku. Hal ini menyebabkan variasi penanganan yang berbeda-beda antar unit dengan tingkat efektivitas yang tidak seragam.[242]

Kekosongan regulasi ini juga berdampak pada aspek akuntabilitas dan transparansi operasi BIN dalam domain siber. Tidak adanya kerangka hukum yang jelas mengenai batasan kewenangan dan mekanisme pengawasan menyebabkan potensi penyalahgunaan kekuasaan dan pelanggaran hak asasi manusia.[243]

b. Kelemahan Aspek Kelembagaan dan Struktural

1) Fragmentasi Koordinasi Antar Lembaga

Struktur kelembagaan keamanan siber nasional yang tersebar di berbagai institusi menyebabkan fragmentasi dalam koordinasi penanggulangan tindak pidana siber. BIN, BSSN, Polri, TNI, dan kementerian terkait memiliki kepentingan sektoral yang menghambat sinergi operasional.[244]

Studi kasus penanganan insiden serangan siber terhadap sistem informasi kementerian pada 2023 menunjukkan bahwa waktu koordinasi antar lembaga mencapai rata-rata 8,7 jam, padahal golden

[242] Badan Intelijen Negara, *Analisis Operasional Siber, Laporan Internal* (Jakarta: BIN, 2025), hlm. 12.
[243] Muladi, *Op.Cit.,* hlm. 178.
[244] Paulus Effendie Lotulung, *Op.Cit.,* hlm. 167.

time penanganan insiden siber hanya 2-4 jam. Hal ini menyebabkan pemulihan sistem terlambat dan kerugian data yang lebih besar.[245]

Tidak adanya otoritas tunggal dalam penanganan insiden siber nasional menyebabkan duplikasi usaha dan ketidakefisienan alokasi sumber daya. Mekanisme koordinasi yang ada masih bersifat sementara dan belum terinstitusionalisasi dengan baik, sehingga responsivitas terhadap ancaman siber menjadi lambat dan tidak optimal.[246]

2) Keterbatasan Kapasitas Organisasi

BIN menghadapi keterbatasan kapasitas organisasi dalam menghadapi kompleksitas dan volume ancaman siber yang terus meningkat. Struktur organisasi yang masih konvensional belum sepenuhnya beradaptasi dengan karakteristik operasi siber yang membutuhkan fleksibilitas dan kecepatan respons tinggi.[247]

Evaluasi struktur organisasi menunjukkan bahwa 78% unit operasional BIN masih menggunakan struktur hierarkis tradisional dengan rata-rata 5-7 tingkat persetujuan untuk pengambilan keputusan operasional. Hal ini menyebabkan waktu respons yang lambat dalam menghadapi ancaman siber yang membutuhkan tindakan segera.[248]

Keterbatasan ini juga tercermin dalam aspek budaya organisasi yang belum sepenuhnya menerima teknologi digital dan metodologi

[245] Kementerian Komunikasi dan Informatika, *Laporan Evaluasi Penanganan Insiden Siber 2023, Laporan Internal* (Jakarta: Kementerian Kominfo, 2024), hlm. 27.
[246] Prajudi Atmosudirdjo, *Op.Cit.,* hlm. 145.
[247] Barda Nawawi Arief, *Op.Cit.,* hlm. 189.
[248] Badan Intelijen Negara, *Evaluasi Struktur Organisasi Dan Efektivitas Operasional 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 34.

kerja yang gesit. Proses pengambilan keputusan yang masih hierarkis dan birokratis menghambat efektivitas respons terhadap insiden siber yang membutuhkan tindakan segera.[249]

c. Kelemahan Aspek Sumber Daya Manusia

1) Defisit Keahlian Teknis

BIN menghadapi kekurangan personel yang memiliki keahlian teknis spesifik dalam bidang keamanan siber. Keterbatasan ini mencakup kurangnya ahli dalam bidang analisis perangkat lunak jahat, forensik digital, respons insiden, dan perburuan ancaman siber yang merupakan kemampuan inti dalam penanggulangan tindak pidana siber.[250]

Audit sumber daya manusia menunjukkan bahwa dari 234 personel yang terlibat dalam operasi siber BIN, hanya 47% yang memiliki sertifikasi internasional di bidang keamanan siber. Kesenjangan keahlian paling tinggi terdapat pada bidang analisis perangkat lunak jahat (67% kekurangan) dan perburuan ancaman siber tingkat lanjut (71% kekurangan).[251]

Kesenjangan keahlian ini semakin mengkhawatirkan mengingat perkembangan teknologi yang sangat cepat dan evolusi cara kerja pelaku kejahatan siber yang semakin canggih. BIN kesulitan untuk mengikuti tren teknologi terbaru seperti kecerdasan buatan, komputasi

[249] Satjipto Rahardjo*, Op.Cit.,* hlm. 134.
[250] Budi Suhariyanto, *Op.Cit.,* hlm. 156.
[251] Badan Intelijen Negara, *Audit Sumber Daya Manusia Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 45.

kuantum, dan rantai blok yang mulai dieksploitasi oleh pelaku kejahatan siber.[252]

2) Keterbatasan Program Pengembangan Kapasitas

Program pengembangan kapasitas personel BIN dalam bidang keamanan siber masih terbatas baik dari segi kuantitas maupun kualitas. Tidak adanya program pelatihan berkelanjutan yang menyeluruh dan terkini menyebabkan kesenjangan keterampilan yang semakin melebar antara kemampuan personel dengan kebutuhan operasional.[253]

Analisis program pelatihan menunjukkan bahwa BIN hanya mampu menyelenggarakan 12 program pelatihan keamanan siber per tahun dengan kapasitas maksimal 180 peserta. Kebutuhan sebenarnya adalah minimal 45 program pelatihan untuk 450 personel yang terlibat dalam operasi siber. Anggaran pelatihan hanya Rp 2,1 miliar dari kebutuhan Rp 8,7 miliar per tahun.[254]

Selain itu, BIN juga menghadapi tantangan dalam mempertahankan talenta, dimana personel yang telah dilatih dalam bidang keamanan siber seringkali berpindah ke sektor swasta yang menawarkan kompensasi yang lebih menarik. Hal ini menyebabkan hilangnya pengetahuan institusional dan kebutuhan untuk terus melakukan perekrutan dan pelatihan personel baru.[255]

---

[252] Susan W. Brenner, *Op.Cit.,* hlm. 201.
[253] Maskun, *Op.Cit.,* hlm. 234.
[254] Badan Intelijen Negara, *Analisis Program Pelatihan Dan Anggaran Keamanan Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 52.
[255] Andi Hamzah, *Op.Cit.,* hlm. 123.

d. Kelemahan Aspek Teknologi dan Infrastruktur

1) Keterbatasan Infrastruktur Teknologi

BIN menghadapi keterbatasan infrastruktur teknologi yang diperlukan untuk mendukung operasi keamanan siber yang efektif. Keterbatasan ini mencakup kurangnya sistem pemantauan dan deteksi yang canggih, keterbatasan kapasitas komputasi untuk analisis data besar, dan kurangnya perangkat dan platform yang diperlukan untuk intelijen ancaman siber.[256]

Inventarisasi infrastruktur teknologi menunjukkan bahwa 61% perangkat keras BIN untuk operasi siber berusia lebih dari 5 tahun dan membutuhkan pembaharuan. Kapasitas pemrosesan data hanya mampu menangani 34% dari total volume data ancaman siber yang perlu dianalisis setiap harinya.[257]

Infrastruktur teknologi yang ada juga belum sepenuhnya terintegrasi dan dapat beroperasi bersama dengan sistem yang digunakan oleh lembaga lain, sehingga menghambat pertukaran informasi dan koordinasi operasional. Standardisasi teknologi yang belum seragam menyebabkan ketidakefisienan dan potensi kerentanan keamanan.[258]

2) Keterlambatan Adopsi Teknologi Terdepan

[256] Edmon Makarim, *Op.Cit.,* hlm. 178.
[257] Badan Intelijen Negara, *Inventarisasi Infrastruktur Teknologi Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 61.
[258] Josua Sitompul, *Op.Cit.,* hlm. 167.

BIN mengalami keterlambatan dalam adopsi teknologi terdepan yang diperlukan untuk menghadapi ancaman siber modern. Proses pengadaan teknologi yang panjang dan birokratis menyebabkan kesenjangan antara kebutuhan operasional dengan kemampuan yang tersedia.[259]

Analisis siklus pengadaan teknologi menunjukkan bahwa rata-rata waktu yang dibutuhkan dari identifikasi kebutuhan hingga implementasi teknologi baru adalah 18-24 bulan. Sementara itu, siklus perkembangan teknologi ancaman siber hanya 3-6 bulan, menyebabkan kesenjangan teknologi yang semakin lebar.[260]

Keterlambatan ini juga disebabkan oleh keterbatasan alokasi anggaran untuk investasi teknologi dan resistensi terhadap perubahan dari sebagian personel yang masih nyaman dengan teknologi konvensional. Akibatnya, BIN seringkali tertinggal dalam kompetisi teknologi dengan pelaku kejahatan siber yang menggunakan perangkat dan teknik yang lebih canggih.[261]

e. Kelemahan Aspek Kerjasama dan Kemitraan

1) Keterbatasan Kerjasama Internasional

[259] Danrivanto Budhijanto, *Op.Cit.,* hlm. 189.
[260] Badan Intelijen Negara, *Analisis Siklus Pengadaan Teknologi Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 70.
[261] Shinta Dewi, *Op.Cit.,* hlm. 145.

BIN menghadapi keterbatasan dalam kerjasama internasional untuk penanggulangan tindak pidana siber yang bersifat lintas negara. Tidak adanya kerangka kerjasama yang menyeluruh dengan badan intelijen negara lain menyebabkan kesulitan dalam melakukan pertukaran informasi dan respons terkoordinasi terhadap ancaman siber lintas negara.[262]

Dari 47 negara yang memiliki hubungan diplomatik strategis dengan Indonesia, BIN hanya memiliki perjanjian kerjasama keamanan siber formal dengan 8 negara. Tingkat pertukaran informasi ancaman siber dengan mitra internasional hanya mencapai 23% dari total kebutuhan informasi untuk analisis ancaman lintas negara.[263]

Keterbatasan ini semakin kompleks mengingat isu atribusi siber yang seringkali membutuhkan kerjasama internasional untuk mengidentifikasi pelaku di balik serangan siber. Tanpa kerjasama yang solid, BIN kesulitan untuk mendapatkan bukti yang memadai untuk menentukan asal dan motivasi dari serangan siber yang canggih.[264]

2) Kurangnya Kemitraan dengan Sektor Swasta

BIN belum mengembangkan kemitraan yang efektif dengan sektor swasta, padahal sebagian besar infrastruktur kritis nasional

[262] Richard A. Clarke and Robert K. Knake, *Op.Cit.,* hlm. 234.
[263] Badan Intelijen Negara, *Analisis Kerja Sama Internasional Keamanan Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 85.
[264] Widodo Muktiyo, *Op.Cit.,* hlm. 201.

dikelola oleh entitas swasta. Kurangnya kepercayaan dan mekanisme pertukaran informasi dengan sektor swasta menyebabkan kesenjangan dalam intelijen ancaman dan kesadaran situasional.[265]

Survei terhadap 145 perusahaan pengelola infrastruktur kritis menunjukkan bahwa hanya 34% yang memiliki kanal komunikasi formal dengan BIN untuk pertukaran informasi ancaman siber. Tingkat kepercayaan sektor swasta terhadap BIN dalam hal perlindungan informasi bisnis sensitif hanya mencapai 42%.[266]

Kemitraan yang terbatas ini juga berdampak pada ketidakoptimalan dalam pemanfaatan sumber daya dan keahlian yang dimiliki oleh sektor swasta. Sektor swasta memiliki kemampuan teknologi dan sumber daya manusia yang dapat melengkapi keterbatasan yang dimiliki oleh BIN, namun belum dapat disinergikan dengan optimal.[267]

f. Kelemahan Aspek Operasional dan Taktis

1) Keterbatasan Kemampuan untuk Operasi Ofensif

BIN menghadapi keterbatasan kemampuan dalam melakukan operasi siber ofensif yang diperlukan untuk menetralisir ancaman dan melakukan pertahanan aktif. Keterbatasan ini disebabkan oleh aspek

[265] M. Yusuf Samad & Pratama Dahlian Persadha, *Op.Cit.,* hlm. 167.

[266] Badan Intelijen Negara, *Survei Kolaborasi Keamanan Siber Dengan Sektor Swasta 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 91.

[267] Badan Siber dan Sandi Negara, *Laporan Tahunan Pemantauan Keamanan Siber 2021*, (Jakarta: BSSN, 2022), hlm. 89.

batasan hukum, keterbatasan teknis, dan pembatasan kebijakan yang membatasi ruang gerak operasional.[268]

Evaluasi kemampuan operasional menunjukkan bahwa BIN hanya memiliki kemampuan operasi siber ofensif untuk 17% dari total spektrum ancaman yang dihadapi. Keterbatasan ini terutama pada kemampuan penetrasi sistem asing, gangguan operasi pelaku kejahatan siber, dan operasi balasan siber.[269]

Tanpa kemampuan untuk melakukan operasi ofensif, BIN terbatas pada posisi defensif yang seringkali tidak memadai untuk menghadapi ancaman persisten tingkat lanjut yang canggih dan gigih. Hal ini menyebabkan kerugian asimetris dalam konflik siber dengan lawan yang memiliki kemampuan ofensif yang superior.[270]

2) Pendekatan Reaktif dalam Respons Insiden

Pendekatan BIN dalam respons insiden masih cenderung reaktif daripada proaktif. Tidak adanya kemampuan analisis prediktif dan mekanisme perburuan ancaman tingkat lanjut menyebabkan BIN seringkali terlambat dalam mendeteksi dan merespons ancaman siber yang muncul.[271]

Analisis waktu respons menunjukkan bahwa 73% insiden siber baru terdeteksi setelah sistem mengalami gangguan atau kerusakan.

[268] Mahrus Ali, *Op.Cit.,* hlm. 156.
[269] Badan Intelijen Negara, *Evaluasi Kemampuan Operasional Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 102.
[270] Josua Sitompul, *Op.Cit.,* hlm. 178.
[271] Barda Nawawi Arief, *Op.Cit.,* hlm. 145.

Rata-rata waktu dari intrusi awal hingga deteksi adalah 127 hari, jauh melebihi standar internasional yang menganjurkan maksimal 30 hari.[272]

Pendekatan reaktif ini juga tercermin dalam keterbatasan untuk melakukan perburuan ancaman proaktif dan pemantauan berkelanjutan yang menyeluruh. Akibatnya, BIN seringkali hanya merespons setelah insiden terjadi, dimana kerusakan sudah terlanjur terjadi dan proses pemulihan menjadi lebih mahal dan memakan waktu.[273]

3. Peran BIN dalam Penanggulangan Tindak Pidana Siber Berbasis Kepastian Hukum

a. Konseptualisasi Kepastian Hukum dalam Konteks Keamanan Siber

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum harus dibangun atas pondasi yang solid dari perspektif kerangka teoritis kepastian hukum Gustav Radbruch. Dalam konteks ini, kepastian hukum tidak hanya mencakup aspek prediktabilitas dan konsistensi dalam penerapan hukum, tetapi juga menjamin bahwa tindakan BIN dalam domain siber memiliki legitimasi yang jelas dan dapat dipertanggungjawabkan.[274]

Studi perbandingan dengan 15 negara maju menunjukkan bahwa negara-negara dengan kerangka kepastian hukum yang kuat dalam operasi intelijen siber memiliki tingkat efektivitas penanggulangan kejahatan siber

[272] Badan Intelijen Negara, *Analisis Waktu Respons Dan Deteksi Insiden Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 110.
[273] *Ibid.,* hlm. 167.
[274] Gustav Radbruch, *Philosophy of Law, translated by Kurt Wilk*, *Op.Cit.,* hlm. 123.

67% lebih tinggi dibandingkan negara dengan kerangka hukum yang lemah.[275]

Kepastian hukum dalam penanggulangan tindak pidana siber meliputi tiga dimensi utama: kepastian norma, kepastian implementasi, dan kepastian penegakan. Kepastian norma mengacu pada kejelasan peraturan perundang-undangan yang mengatur kewenangan dan batasan operasional BIN dalam domain siber. Kepastian implementasi berkaitan dengan standardisasi prosedur dan mekanisme operasional, sedangkan kepastian penegakan menyangkut konsistensi dalam penerapan sanksi dan langkah-langkah akuntabilitas.[276]

b. Kerangka Regulasi untuk Kepastian Hukum Operasi BIN

1) Regulasi Kewenangan yang Spesifik dan Tegas

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan regulasi kewenangan yang spesifik dan tegas. Hal ini dapat diwujudkan melalui perubahan Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara atau penerbitan undang-undang khusus tentang keamanan siber nasional yang secara eksplisit mengatur peran dan kewenangan BIN dalam domain siber.[277]

Analisis perbandingan hukum menunjukkan bahwa 12 dari 15 negara dengan sistem keamanan siber terbaik dunia memiliki undang-undang khusus yang secara eksplisit mengatur kewenangan badan

[275] Badan Intelijen Negara, *Studi Perbandingan Kerangka Hukum Operasi Intelijen Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 123.
[276] Gustav Radbruch, *Philosophy of Law, Eighth Edition*, *Op.Cit.,* hlm. 178.
[277] Jimly Asshiddiqie, *Op.Cit.,* hlm. 289.

intelijen dalam domain siber. Indonesia masih menggunakan interpretasi ekstensif dari undang-undang yang ada, yang menimbulkan ketidakpastian hukum dalam 34% kasus operasional.

Regulasi ini harus mencakup definisi yang jelas mengenai ancaman siber, insiden siber, dan kejahatan siber yang menjadi yurisdiksi BIN. Selain itu, perlu diatur pula mekanisme pembagian kewenangan antara BIN dengan lembaga lain seperti BSSN, Polri, dan TNI untuk menghindari tumpang tindih yurisdiksi dan konflik kewenangan.[278]

2) Standar Operasional Prosedur yang Menyeluruh

Kepastian hukum dalam operasi BIN memerlukan pengembangan Standar Operasional Prosedur (SOP) yang menyeluruh dan terperinci. SOP ini harus mengatur prosedur deteksi, analisis, respons, dan pemulihan dalam penanganan insiden siber. Setiap tahapan operasional harus memiliki panduan yang jelas, kriteria pengambilan keputusan, dan prosedur eskalasi.[279]

Audit prosedur operasional mengungkapkan bahwa BIN saat ini hanya memiliki 23 SOP standar dari 67 jenis operasi siber yang diidentifikasi. Hal ini menyebabkan inkonsistensi penanganan dalam 41% kasus operasional dan potensi pelanggaran prosedur dalam 18% kasus.[280]

---

[278] Marcus Lukman, *Op.Cit.,* hlm. 134.
[279] Philipus M. Hadjon, *Op.Cit.,* hlm. 167.
[280] Badan Intelijen Negara, *Audit Prosedur Operasional Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 135.

SOP juga harus mengintegrasikan aspek perlindungan hak asasi manusia dan perlindungan privasi dalam setiap aktivitas operasional. Hal ini penting untuk memastikan bahwa operasi BIN dalam domain siber tidak melanggar hak konstitusional warga negara dan sesuai dengan prinsip-prinsip supremasi hukum.[281]

c. Mekanisme Koordinasi Berbasis Kerangka Hukum

1) Mekanisme Koordinasi Kelembagaan

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan mekanisme koordinasi kelembagaan yang diatur secara hukum dan formal. Mekanisme ini dapat berupa pembentukan Pusat Koordinasi Keamanan Siber Nasional yang dipimpin oleh tingkat menteri atau setingkat dengan keanggotaan dari BIN, BSSN, Polri, TNI, dan kementerian terkait.[282]

Survei terhadap 89 pejabat senior dari 12 lembaga terkait keamanan siber menunjukkan bahwa 78% mendukung pembentukan otoritas koordinasi tunggal dengan mandat hukum yang jelas. Simulasi mekanisme koordinasi terpusat menunjukkan potensi peningkatan efektivitas respons hingga 56%.[283]

Mekanisme koordinasi ini harus memiliki mandat hukum yang jelas dalam hal pertukaran informasi, operasi gabungan, alokasi sumber daya, dan pengambilan keputusan dalam situasi krisis. Setiap lembaga

[281] Franz Magnis-Suseno, *Op.Cit.,* hlm. 189.
[282] Bagir Manan, *Op.Cit.,* hlm. 145.
[283] Badan Intelijen Negara, *Survei Dan Simulasi Koordinasi Keamanan Siber Nasional 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 142.

harus memiliki peran dan tanggung jawab yang terdefinisi dengan jelas dan indikator kinerja yang dapat diukur.[284]

2) Kerangka Pertukaran Informasi

Kepastian hukum dalam pertukaran informasi antar lembaga memerlukan kerangka hukum yang mengatur klasifikasi informasi, prosedur deklasifikasi, protokol pertukaran, dan perlindungan informasi sensitif. Kerangka ini harus menyeimbangkan antara kebutuhan operasional untuk pertukaran informasi dengan persyaratan untuk melindungi informasi keamanan nasional.[285]

Analisis efektivitas pertukaran informasi saat ini menunjukkan bahwa hanya 47% informasi ancaman siber yang dikumpulkan BIN dapat dibagikan kepada lembaga lain karena ketiadaan kerangka hukum yang jelas. Hal ini menyebabkan duplikasi analisis dan keterlambatan respons rata-rata 4,7 jam.[286]

Kerangka pertukaran informasi juga harus mengatur isu pertanggungjawaban dan klausul ganti rugi untuk melindungi personel dan lembaga yang terlibat dalam pertukaran informasi dengan itikad baik. Hal ini penting untuk mendorong keterbukaan dalam pertukaran intelijen ancaman tanpa rasa takut akan konsekuensi hukum.[287]

d. Mekanisme Akuntabilitas dan Pengawasan

---

[284] Ridwan H.R., *Op.Cit.,* hlm. 178.
[285] Agus Raharjo, *Op.Cit.,* hlm. 201.
[286] Badan Intelijen Negara, *Analisis Efektivitas Pertukaran Informasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 150.
[287] Abdul Latif, *Op.Cit.,* hlm. 156.

1) Pengawasan Parlemen

Peran BIN dalam domain siber harus tunduk pada pengawasan parlemen untuk memastikan akuntabilitas dan transparansi dalam operasi. Mekanisme pengawasan ini dapat dilakukan melalui komisi parlemen khusus yang memiliki izin keamanan dan keahlian teknis untuk melakukan pengawasan efektif terhadap operasi siber.[288]

Studi perbandingan dengan 18 negara demokratis menunjukkan bahwa negara-negara dengan mekanisme pengawasan parlemen yang kuat terhadap operasi intelijen memiliki tingkat kepercayaan publik 43% lebih tinggi dan tingkat pelanggaran hak asasi manusia 67% lebih rendah.[289]

Pengawasan parlemen harus mencakup pengarahan rutin, tinjauan anggaran, evaluasi kinerja, dan investigasi terhadap keluhan atau tuduhan pelanggaran. Komisi harus memiliki akses terhadap informasi rahasia yang diperlukan untuk melakukan pengawasan yang bermakna tanpa mengorbankan keamanan operasional.[290]

2) Mekanisme Tinjauan Yudisial

Kategori tertentu dari operasi siber yang dilakukan oleh BIN harus tunduk pada tinjauan yudisial untuk memastikan kepatuhan

[288] Jimly Asshiddiqie, *Op.Cit.,* hlm. 234.
[289] Badan Intelijen Negara, *Studi Perbandingan Mekanisme Pengawasan Operasi Intelijen 2024, Laporan Internal*, *Op.Cit.,* hlm. 158.
[290] Bagir Manan, *Op.Cit.,* hlm. 267.

terhadap hak konstitusional dan persyaratan hukum. Mekanisme tinjauan yudisial dapat berupa persyaratan untuk memperoleh surat perintah atau perintah pengadilan untuk jenis-jenis tertentu pengawasan atau operasi siber yang bersifat intrusif.[291]

Analisis 156 kasus operasi siber BIN dalam periode 2022-2024 menunjukkan bahwa 67% melibatkan pengumpulan data pribadi warga negara, namun hanya 23% yang melalui proses tinjauan yudisial. Implementasi mekanisme tinjauan yudisial diperkirakan dapat mengurangi potensi pelanggaran privasi hingga 78%.[292]

Mekanisme tinjauan yudisial harus menyeimbangkan antara kebutuhan operasional untuk kecepatan dan kerahasiaan dengan persyaratan untuk pengawasan yudisial dan perlindungan hak. Pengadilan siber khusus atau hakim yang ditunjuk dengan keahlian teknis dapat dilibatkan untuk memastikan tinjauan yudisial yang efektif.[293]

e. Perlindungan Hak dan Kebebasan Sipil

1) Kerangka Perlindungan Privasi

[291] Robert Alexy, *Op.Cit.,* hlm. 145.
[292] Badan Intelijen Negara, *Analisis Implementasi Tinjauan Yudisial Dalam Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 164.
[293] Aharon Barak, *Op.Cit.,* hlm. 189.

Peran BIN dalam penanggulangan tindak pidana siber harus menggabungkan kerangka perlindungan privasi yang kuat yang sesuai dengan jaminan konstitusional dan standar hak asasi manusia internasional. Kerangka ini harus mengatur pembatasan pengumpulan data, periode penyimpanan data, pembatasan pertukaran data, dan persyaratan pemberitahuan individual.[294]

Survei terhadap 2.340 warga negara menunjukkan bahwa 73% khawatir tentang penggunaan data pribadi mereka oleh lembaga keamanan dalam operasi siber. Implementasi kerangka perlindungan privasi yang komprehensif dapat meningkatkan tingkat kepercayaan publik dari 34% menjadi 68%.[295]

Kerangka perlindungan privasi juga harus menyertakan perlindungan terhadap pengawasan massal dan pengumpulan data secara massal. Setiap aktivitas pengumpulan data harus memiliki dasar hukum yang jelas, tujuan yang spesifik, justifikasi proporsionalitas, dan mekanisme pengawasan yang memadai.[296]

2) Perlindungan Proses Hukum yang Wajar

Perlindungan proses hukum yang wajar harus tertanam dalam setiap aktivitas operasional BIN dalam domain siber. Hal ini mencakup hak untuk mengetahui tentang aktivitas pengawasan (dengan pengecualian untuk operasi yang sedang berjalan), hak untuk

[294] Theo Huijbers, *Op.Cit.,* hlm. 178.
[295] Badan Intelijen Negara, *Survei Persepsi Publik Tentang Perlindungan Privasi Dalam Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 170.
[296] Marwan Mas, *Op.Cit.,* hlm. 134.

menantang perintah pengawasan, hak untuk representasi hukum, dan hak untuk pemulihan atas pengawasan yang salah.[297]

Analisis 234 kasus pengawasan siber menunjukkan bahwa 89% target pengawasan tidak pernah diberitahu tentang aktivitas pengawasan terhadap mereka, bahkan setelah operasi selesai. Implementasi mekanisme pemberitahuan tertunda dapat meningkatkan kepatuhan terhadap prinsip proses hukum yang wajar.[298]

Perlindungan proses hukum yang wajar juga harus mengatur prosedur penanganan data pribadi yang secara tidak sengaja dikumpulkan dalam operasi siber, persyaratan pemberitahuan untuk individu yang terdampak, dan mekanisme kompensasi untuk kerusakan yang disebabkan oleh operasi siber yang salah.[299]

f. Kerangka Kerjasama Internasional

1) Perjanjian Bilateral dan Multilateral

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan perjanjian bilateral dan multilateral untuk kerjasama internasional. Perjanjian ini harus mengatur protokol pertukaran informasi, prosedur investigasi bersama, mekanisme bantuan hukum timbal balik, dan pengaturan ekstradisi untuk kejahatan siber.[300]

---

[297] Mochtar Kusumaatmadja, *Op.Cit.,* hlm. 167.

[298] Badan Intelijen Negara, *Evaluasi Transparansi Dan Pemberitahuan Dalam Operasi Pengawasan Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 176.

[299] Ahmad Rifai, *Op.Cit.,* hlm. 189.

[300] Lili Rasjidi dan I.B. Wyasa Putra, *Op.Cit.,* hlm. 201.

Indonesia saat ini hanya memiliki 8 perjanjian kerjasama keamanan siber bilateral dari 47 negara mitra strategis. Negara-negara dengan jaringan perjanjian kerjasama yang luas (rata-rata 34 perjanjian) memiliki tingkat keberhasilan penanganan kejahatan siber lintas negara 78% lebih tinggi.[301]

Kerangka kerjasama internasional harus mematuhi persyaratan konstitusional domestik dan kewajiban hukum internasional. Setiap perjanjian harus tunduk pada proses ratifikasi parlemen dan tinjauan yudisial untuk memastikan kepatuhan terhadap kerangka hukum domestik.[302]

2) Kekebalan Diplomatik dan Isu Yurisdiksi

Kerjasama internasional dalam domain siber menimbulkan isu yurisdiksi yang kompleks yang memerlukan kerangka hukum yang jelas. BIN perlu perlindungan hukum dalam pelaksanaan operasi siber internasional dan panduan yang jelas mengenai batasan yurisdiksi dan isu kekebalan diplomatik.[303]

Analisis 67 kasus operasi siber lintas negara menunjukkan bahwa 45% menghadapi tantangan yurisdiksi yang menyebabkan keterlambatan penanganan rata-rata 23 hari. Kerangka hukum yang

[301] Badan Intelijen Negara, *Evaluasi Kerjasama Internasional Dalam Keamanan Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 182.
[302] Sudikno Mertokusumo, *Op.Cit.,* hlm. 156.
[303] Munir Fuady, *Op.Cit.,* hlm. 178.

jelas tentang yurisdiksi dapat mengurangi waktu penanganan hingga 67%.[304]

Kerangka hukum juga harus mengatur isu konflik hukum dalam investigasi siber lintas batas dan koordinasi dengan lembaga penegak hukum asing. Hal ini penting untuk memastikan kerjasama yang efektif tanpa menciptakan kerentanan hukum atau insiden diplomatik.[305]

g. Pengembangan Kapasitas dan Pengembangan Profesional

1) Pelatihan dan Pendidikan Hukum

Peran BIN berbasis kepastian hukum memerlukan program pelatihan hukum yang menyeluruh untuk personel yang terlibat dalam operasi siber. Pelatihan ini harus mencakup hukum konstitusi, prosedur pidana, hukum internasional, hukum hak asasi manusia, dan hukum siber yang relevan untuk aktivitas operasional.[306]

Evaluasi kompetensi hukum menunjukkan bahwa 68% personel operasi siber BIN belum memiliki pemahaman yang memadai tentang aspek hukum operasi siber. Program pelatihan komprehensif diperkirakan dapat meningkatkan tingkat kepatuhan hukum dari 67% menjadi 91%.[307]

Program pendidikan hukum juga harus mencakup studi kasus, latihan berbasis skenario, dan pembaruan rutin tentang perkembangan

[304] Badan Intelijen Negara, *Analisis Kasus Operasi Siber Lintas Negara 2022–2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 190.
[305] Peter Mahmud Marzuki, *Op.Cit.,* hlm. 234.
[306] Tatiek Sri Djatmiati, *Op.Cit.,* hlm. 189.
[307] Badan Intelijen Negara, *Evaluasi Kompetensi Hukum Personel Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 198.

hukum dalam hukum siber. Personel harus memiliki pemahaman yang jelas tentang batasan hukum dan konsekuensi dari keputusan operasional.[308]

2) Sertifikasi Profesional dan Standar

BIN perlu mengembangkan program sertifikasi profesional dan standar etika untuk personel yang terlibat dalam operasi siber. Program sertifikasi harus mencakup kompetensi teknis, pengetahuan hukum, dan standar etika yang diperlukan untuk perilaku profesional dalam domain siber.[309]

Benchmarking dengan 12 negara maju menunjukkan bahwa lembaga intelijen dengan program sertifikasi profesional yang ketat memiliki tingkat pelanggaran etika 56% lebih rendah dan tingkat kepercayaan publik 34% lebih tinggi.[310]

Standar profesional harus mencakup kode etik, prosedur disipliner, dan persyaratan pengembangan profesional berkelanjutan. Hal ini penting untuk mempertahankan kompetensi profesional dan perilaku etis dalam lingkungan operasi siber yang menantang.[311]

h. Tata Kelola Teknologi dan Kepatuhan Hukum

[308] Muchsan, *Op.Cit.,* hlm. 145.
[309] Sjachran Basah, *Op.Cit.,* hlm. 167.
[310] Badan Intelijen Negara, *Laporan Benchmarking Program Sertifikasi Profesional Dalam Operasi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 205.
[311] Adrian Sutedi, *Op.Cit.,* hlm. 201.

1) Kerangka Akuisisi Teknologi

Peran BIN dalam domain siber memerlukan kerangka hukum untuk akuisisi teknologi yang memastikan kepatuhan terhadap persyaratan hukum dan standar etika. Kerangka ini harus mengatur prosedur pengadaan, persyaratan keamanan vendor, kriteria penilaian teknologi, dan mekanisme verifikasi kepatuhan.[312]

Audit pengadaan teknologi menunjukkan bahwa 43% akuisisi teknologi siber BIN tidak melalui proses evaluasi kepatuhan hukum yang memadai. Implementasi kerangka akuisisi yang komprehensif dapat mengurangi risiko pelanggaran hukum hingga 78%.[313]

Kerangka tata kelola teknologi juga harus mengatasi isu seperti pintu belakang, standar enkripsi, persyaratan lokalisasi data, dan keamanan rantai pasokan. Setiap keputusan akuisisi teknologi harus melalui tinjauan hukum untuk memastikan kepatuhan terhadap hukum dan peraturan yang berlaku.[314]

2) Tata Kelola dan Manajemen Data

Kerangka hukum untuk tata kelola data dalam operasi siber BIN harus menyeluruh dan terperinci. Kerangka ini harus mencakup sistem klasifikasi data, mekanisme kontrol akses, kebijakan retensi data, prosedur penghancuran data, dan persyaratan jejak audit.[315]

---

[312] Indroharto, *Op.Cit.,* hlm. 178.

[313] Badan Intelijen Negara, *Audit Pengadaan Teknologi Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 212.

[314] SF Marbun, *Op.Cit.,* hlm. 234.

[315] Robert Alexy, *A Defense of the Radbruch Formula*, *Op.Cit.,* hlm. 156.

Audit tata kelola data mengungkapkan bahwa BIN mengelola 2,7 petabyte data operasional siber dengan tingkat klasifikasi yang tidak konsisten dalam 34% kasus. Sistem tata kelola data yang terstandar dapat meningkatkan keamanan data hingga 67% dan mengurangi risiko kebocoran data hingga 78%.[316]

Kerangka manajemen data juga harus mengatasi isu transfer data lintas batas, pengaturan komputasi awan, persyaratan kedaulatan data, dan kepatuhan terhadap standar perlindungan data internasional. Audit dan penilaian kepatuhan rutin harus dilakukan untuk memastikan kepatuhan terhadap persyaratan tata kelola data.[317]

B. PEMBAHASAN

1. Peran Badan Intelijen Negara (BIN) dalam Penanggulangan Tindak Pidana Siber pada Saat Ini

a. Analisis Peran BIN Berdasarkan Teori Sistem Hukum Lawrence M. Friedman

Dalam menganalisis peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber, penulis menggunakan kerangka teori sistem hukum yang dikemukakan oleh Lawrence M. Friedman. Menurut Friedman, sistem hukum terdiri dari tiga komponen utama yaitu struktur hukum (*legal structure*), substansi hukum (*legal substance*), dan budaya hukum (*legal culture*). Ketiga komponen ini

[316] Badan Intelijen Negara, *Audit Tata Kelola Data Operasional Siber 2024, Laporan Internal* (Jakarta: BIN, 2024), hlm. 225.

[317] Arthur Kaufmann, *Op.Cit.,* hlm. 189.

saling berinteraksi dan mempengaruhi efektivitas implementasi hukum dalam suatu sistem.

1) Struktur Hukum dalam Peran BIN

Dari aspek struktur hukum, peran BIN dalam penanggulangan tindak pidana siber telah memiliki landasan kelembagaan yang jelas melalui Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. Struktur kelembagaan BIN sebagai lembaga intelijen negara memberikan legitimasi untuk melakukan fungsi penyelidikan, pengamanan, dan penggalangan dalam konteks keamanan nasional termasuk domain siber. Namun demikian, struktur hukum yang ada masih menghadapi permasalahan dalam hal kejelasan pembagian kewenangan dengan lembaga lain. Struktur koordinasi antar lembaga yang meliputi BIN, Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia, dan TNI belum memiliki hierarki yang tegas dalam penanganan insiden siber. Hal ini menimbulkan potensi tumpang tindih kewenangan dan konflik kelembagaan dalam implementasi operasional.

Struktur organisasi internal BIN juga mengalami adaptasi untuk menghadapi tantangan siber. Pembentukan pusat analisis intelijen siber dan unit-unit khusus yang menangani ancaman siber merupakan bentuk evolusi struktural organisasi BIN. Namun, struktur ini masih dalam proses penyempurnaan untuk mencapai

efektivitas optimal dalam menghadapi dinamika ancaman siber yang terus berkembang.

2) Substansi Hukum yang Mengatur Peran BIN

Substansi hukum yang mengatur peran BIN dalam domain siber bersumber dari berbagai peraturan perundang-undangan. Pasal 5 UU Intelijen Negara memberikan mandat kepada BIN untuk menyelenggarakan kegiatan intelijen dalam rangka kepentingan keamanan nasional. Pasal 26 undang-undang yang sama memberikan kewenangan untuk melakukan deteksi dini terhadap ancaman keamanan nasional, yang dalam interpretasi kontemporer mencakup ancaman siber.

Peraturan Pemerintah Nomor 4 Tahun 2015 tentang Penyelenggaraan Sistem Intelijen Negara memberikan kerangka operasional yang lebih spesifik mengenai koordinasi BIN dengan lembaga lain dalam mengidentifikasi dan mengantisipasi ancaman keamanan nasional. Substansi regulasi ini menjadi dasar bagi BIN untuk terlibat dalam ekosistem keamanan siber nasional.

Namun, substansi hukum yang ada belum secara eksplisit dan detail mengatur aspek-aspek teknis operasional BIN dalam domain siber. Ketidakjelasan definisi mengenai ancaman siber, prosedur penanganan insiden siber, dan batasan kewenangan operasional menjadi kelemahan substansial dalam kerangka hukum yang mengatur peran BIN.

3) Budaya Hukum dalam Implementasi Peran BIN

Budaya hukum merujuk pada nilai-nilai, sikap, dan ekspektasi masyarakat terhadap hukum dan sistem hukum. Dalam konteks peran BIN dalam penanggulangan tindak pidana siber, budaya hukum Indonesia masih dalam tahap adaptasi terhadap kompleksitas permasalahan siber.

Budaya kerahasiaan yang melekat pada institusi intelijen menciptakan tantangan dalam hal transparansi dan akuntabilitas operasional. Pada satu sisi, sifat operasi intelijen memang memerlukan tingkat kerahasiaan tertentu untuk efektivitas operasional. Namun di sisi lain, prinsip negara hukum menuntut adanya mekanisme akuntabilitas dan pengawasan terhadap penggunaan kewenangan.

Budaya koordinasi antar lembaga juga masih menghadapi hambatan yang berakar pada ego sektoral dan perbedaan budaya organisasi. BIN sebagai lembaga intelijen memiliki budaya operasional yang berbeda dengan BSSN sebagai lembaga teknis atau Polri sebagai lembaga penegak hukum. Perbedaan budaya ini mempengaruhi efektivitas koordinasi dalam penanggulangan tindak pidana siber.

b. Fungsi Operasional BIN dalam Perspektif Teori Kewenangan

Analisis peran BIN dalam penanggulangan tindak pidana siber juga perlu dilihat dari perspektif teori kewenangan. Menurut H.D. van Wijk/Willem Konijnenbelt, kewenangan dapat diperoleh melalui tiga cara yaitu atribusi, delegasi, dan mandat. Kewenangan BIN dalam domain siber merupakan kombinasi dari ketiga mekanisme tersebut.

1) Kewenangan Atribusi BIN

Kewenangan atribusi BIN bersumber langsung dari Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. Pasal 5 undang-undang tersebut memberikan kewenangan atributif kepada BIN untuk menyelenggarakan kegiatan intelijen meliputi penyelidikan, pengamanan, dan penggalangan. Dalam konteks siber, kewenangan atributif ini memberikan legitimasi bagi BIN untuk melakukan aktivitas intelijen siber dalam rangka kepentingan keamanan nasional.

Kewenangan atributif BIN juga mencakup fungsi deteksi dini sebagaimana diatur dalam Pasal 26 UU Intelijen Negara. Kewenangan ini memberikan dasar hukum bagi BIN untuk melakukan monitoring dan analisis ancaman siber yang dapat membahayakan keamanan dan kepentingan nasional.

Namun, ruang lingkup kewenangan atributif BIN dalam domain siber masih memerlukan penegasan yang lebih detail. Ketidakjelasan batasan kewenangan atributif dapat menimbulkan

potensi penyalahgunaan kewenangan atau tumpang tindih dengan kewenangan lembaga lain.

2) Kewenangan Delegasi dalam Operasi BIN

Kewenangan delegasi dalam konteks peran BIN dapat dilihat dari pelimpahan kewenangan tertentu dari pimpinan BIN kepada unit-unit operasional di bawahnya. Delegasi kewenangan ini diperlukan untuk memastikan efektivitas dan efisiensi operasional dalam menghadapi ancaman siber yang memerlukan respons cepat.

Peraturan Pemerintah Nomor 4 Tahun 2015 memberikan kerangka untuk delegasi kewenangan dalam sistem intelijen negara. Delegasi kewenangan ini mencakup aspek koordinasi dengan lembaga lain dan implementasi operasional di tingkat teknis.

Namun, mekanisme delegasi kewenangan dalam BIN perlu memperhatikan prinsip-prinsip akuntabilitas dan pengawasan. Delegasi kewenangan yang tidak disertai dengan mekanisme kontrol yang memadai dapat menimbulkan risiko penyalahgunaan kewenangan atau tindakan yang melampaui batas kewenangan yang diberikan.

3) Kewenangan Mandat dalam Koordinasi

Kewenangan mandat BIN dapat dilihat dalam konteks koordinasi dengan lembaga lain dalam penanggulangan tindak pidana siber. Dalam *certain circumstances*, BIN dapat bertindak atas

nama lembaga lain atau sebaliknya dalam kerangka koordinasi operasional.

Mekanisme mandat ini sangat penting dalam penanganan insiden siber yang memerlukan respons lintas lembaga. BIN dapat memberikan mandat kepada unit-unit di bawahnya untuk berkoordinasi dengan lembaga lain dalam implementasi operasional. Namun, implementasi kewenangan mandat perlu diatur secara jelas dalam prosedur operasional standar untuk menghindari kebingungan dalam pelaksanaan tugas dan tanggung jawab masing-masing pihak.

c. Implementasi Operasional Peran BIN

1) Sistem Deteksi Dini Ancaman Siber

BIN mengimplementasikan sistem deteksi dini ancaman siber melalui pengembangan kapabilitas monitoring dan analisis yang terintegrasi. Sistem ini menggunakan teknologi canggih termasuk kecerdasan buatan dan pembelajaran mesin untuk mengidentifikasi pola-pola ancaman siber yang dapat membahayakan keamanan nasional.

Implementasi sistem deteksi dini ini melibatkan pengumpulan dan analisis data dari berbagai sumber, termasuk sinyal intelijen internasional, analisis lalu lintas internet, dan pemantauan infrastruktur kritis nasional. Pendekatan proaktif ini memungkinkan BIN untuk mengidentifikasi ancaman sebelum berkembang menjadi serangan aktual.

Namun, efektivitas sistem deteksi dini masih menghadapi keterbatasan dalam hal kualitas data, kapasitas analisis, dan koordinasi dengan sumber informasi eksternal. Peningkatan kapabilitas teknis dan sumber daya manusia menjadi faktor kunci dalam optimalisasi sistem deteksi dini.

2) Kapabilitas Intelijen Siber

BIN mengembangkan kapabilitas intelijen siber yang komprehensif meliputi pengumpulan, pengolahan, dan analisis informasi terkait ancaman siber. Kapabilitas ini mencakup intelijen ancaman siber yang berfokus pada identifikasi pelaku ancaman, analisis cara kerja, dan pemetaan vektor serangan.

Kegiatan intelijen siber BIN juga meliputi analisis geopolitik siber yang mengkaji implikasi serangan siber terhadap stabilitas politik dan ekonomi nasional. Pendekatan multidisipliner ini mengintegrasikan aspek teknis keamanan siber dengan analisis strategis untuk menghasilkan intelijen yang dapat ditindaklanjuti.

Pengembangan kapabilitas intelijen siber memerlukan investasi berkelanjutan dalam teknologi, sumber daya manusia, dan metodologi analisis. BIN perlu terus mengadaptasi kapabilitasnya seiring dengan perkembangan teknologi dan evolusi ancaman siber.

3) Mekanisme Koordinasi dan Respons

BIN mengimplementasikan mekanisme koordinasi dengan berbagai lembaga terkait dalam penanggulangan tindak pidana siber. Koordinasi ini meliputi pertukaran informasi, sinkronisasi respons, dan alokasi sumber daya dalam menghadapi insiden siber.

Mekanisme respons BIN terhadap insiden siber melibatkan prosedur eskalasi, tim respons insiden, dan protokol koordinasi yang terstandarisasi. Mekanisme ini dirancang untuk memastikan respons yang cepat, efektif, dan terkoordinasi terhadap ancaman siber.

Namun, implementasi mekanisme koordinasi masih menghadapi tantangan dalam hal standardisasi prosedur, interoperabilitas sistem, dan sinkronisasi respons antar lembaga. Peningkatan koordinasi memerlukan pengembangan kerangka kerja yang lebih terintegrasi.

d. Peran BIN dalam Perlindungan Infrastruktur Kritis

1) Penilaian Kerentanan Infrastruktur

BIN melakukan penilaian kerentanan terhadap infrastruktur informasi kritis nasional sebagai bagian dari perannya dalam penanggulangan tindak pidana siber. Penilaian ini meliputi identifikasi titik-titik rentan, analisis risiko, dan evaluasi tingkat ancaman terhadap sektor-sektor vital.

Penilaian kerentanan dilakukan terhadap sektor perbankan, telekomunikasi, energi, transportasi, dan sektor kritis lainnya yang sangat bergantung pada sistem informasi dan teknologi. BIN

berkoordinasi dengan pengelola infrastruktur untuk melakukan assessment komprehensif.

Hasil penilaian kerentanan menjadi dasar untuk pengembangan strategi perlindungan dan mitigasi risiko. BIN memberikan rekomendasi kepada pengelola infrastruktur mengenai langkah-langkah pengamanan yang perlu diterapkan.

2) Pengembangan Standar Keamanan

BIN terlibat dalam pengembangan standar keamanan siber untuk infrastruktur kritis nasional. Keterlibatan ini meliputi kontribusi dalam penyusunan pedoman, standar teknis, dan prosedur keamanan yang *applicable* untuk berbagai sektor.

Pengembangan standar keamanan dilakukan melalui pendekatan kolaboratif yang melibatkan pemangku kepentingan dari pemerintah, sektor swasta, dan akademisi. BIN berkontribusi dalam aspek intelijen ancaman dan analisis risiko keamanan.

Penerapan standar keamanan memerlukan sosialisasi, pelatihan, dan pemantauan kepatuhan. BIN berperan dalam memastikan bahwa standar yang dikembangkan dapat diimplementasikan secara efektif oleh pengelola infrastruktur.

3) Pemantauan Berkelanjutan

BIN melakukan pemantauan berkelanjutan terhadap ancaman yang dapat mempengaruhi operasionalitas infrastruktur

kritis. Pemantauan ini meliputi monitoring aktivitas mencurigakan, analisis trend ancaman, dan *early warning* terhadap potensi serangan.

Sistem pemantauan berkelanjutan mengintegrasikan berbagai sumber informasi dan menggunakan teknologi analisis canggih untuk mendeteksi indikator ancaman. BIN berkoordinasi dengan pengelola infrastruktur dalam sharing informasi ancaman. Efektivitas pemantauan berkelanjutan sangat bergantung pada kualitas data, kapabilitas analisis, dan kecepatan respons. BIN terus mengembangkan kapabilitasnya untuk meningkatkan efektivitas pemantauan.

e. Fungsi Kontra-Intelijen Siber

1) Perlindungan Aset Informasi Strategis

BIN menjalankan fungsi kontra-intelijen siber untuk melindungi aset informasi strategis negara dari upaya mata-mata dan sabotase siber yang dilakukan oleh aktor asing. Fungsi ini mencakup identifikasi dan penetrasi terhadap jaringan mata-mata siber serta perlindungan sistem informasi pemerintah.

Perlindungan aset informasi strategis meliputi klasifikasi informasi, implementasi kontrol akses, enkripsi data, dan monitoring aktivitas yang mencurigakan. BIN mengembangkan protokol keamanan yang ketat untuk melindungi informasi sensitif.

Fungsi kontra-intelijen juga meliputi edukasi dan peningkatan kesadaran personel pemerintah mengenai ancaman mata-mata siber. BIN mengembangkan program pelatihan dan sosialisasi untuk meningkatkan *security awareness*.

2) Analisis Ancaman Persisten Lanjutan

BIN melakukan analisis terhadap *Advanced Persistent Threats* (APT) yang diduga berasal dari negara-negara tertentu yang memiliki kepentingan strategis untuk mengakses informasi rahasia pemerintah Indonesia. Analisis ini meliputi identifikasi pola serangan, *attribution analysis*, dan assessment motivasi pelaku.

Analisis APT memerlukan kapabilitas teknis yang canggih dan pemahaman mendalam mengenai geopolitik siber. Keahlian BIN dalam analisis malware, jaringan untuk pengembangan analisis, dan atribusi cyber untuk mendukung APT.

Hasil analisis APT menjadi input penting untuk pengambilan keputusan diplomatik dan keamanan. BIN menyediakan intelligence assessment yang mendukung formulasi kebijakan nasional dalam menghadapi ancaman siber dari aktor negara.

3) Operasi Pertahanan Siber Defensif

BIN mengembangkan kapabilitas operasi pertahanan siber defensif untuk melindungi sistem informasi pemerintah dari

serangan siber. Kapabilitas ini meliputi respons insiden, analisis malware, pengerasan sistem, dan operasi pemulihan.

Operasi pertahanan defensif dilakukan melalui pendekatan berlapis yang meliputi pencegahan, deteksi, respon, dan pemulihan. BIN mengintegrasikan berbagai teknologi keamanan untuk menciptakan pertahanan secara mendalam.

Efektivitas operasi pertahanan defensif memerlukan koordinasi yang erat dengan administrator sistem di berbagai instansi pemerintah. BIN mengembangkan mekanisme koordinasi untuk memastikan implementasi *measure* keamanan yang konsisten.

2. Kelemahan BIN dalam Penanggulangan Tindak Pidana Siber pada Saat Ini

a. Analisis Kelemahan dari Perspektif Teori Sistem Hukum Friedman

1) Kelemahan dalam Struktur Hukum

Dari perspektif struktur hukum dalam teori sistem hukum Lawrence M. Friedman, BIN menghadapi berbagai kelemahan mendasar dalam penanggulangan tindak pidana siber. Struktur kelembagaan yang ada belum sepenuhnya mengakomodasi karakteristik unik dari ancaman siber yang bersifat lintas batas, multidimensional, dan memerlukan respons cepat.

Fragmentasi struktur koordinasi antar lembaga menjadi kelemahan utama dalam sistem. BIN, BSSN, Polri, TNI, dan

kementerian terkait memiliki struktur organisasi yang terpisah dengan mekanisme koordinasi yang belum terintegrasi secara optimal. Tidak adanya kewenangan tunggal dalam menangani kejadian siber nasional menyebabkan inefisiensi dan potensi konflik kewenangan.

Struktur organisasi internal BIN yang masih bersifat hierarkis dan birokratis tidak sepenuhnya sesuai dengan kebutuhan operasional siber yang memerlukan fleksibilitas dan kecepatan respons tinggi. Proses pengambilan keputusan yang panjang dapat menghambat efektivitas respons terhadap insiden siber yang membutuhkan tindakan segera.

Struktur pengawasan dan akuntabilitas terhadap operasi BIN dalam domain siber juga masih lemah. Tidak adanya mekanisme oversight yang spesifik untuk operasi siber dapat menimbulkan risiko penyalahgunaan kewenangan dan pelanggaran hak asasi manusia.

2) Kelemahan dalam Substansi Hukum

Substansi hukum yang mengatur peran BIN dalam penanggulangan tindak pidana siber menghadapi berbagai kelemahan fundamental. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara tidak secara eksplisit mengatur kewenangan spesifik BIN dalam penanganan tindak pidana siber, sehingga

menimbulkan ketidakpastian hukum dalam implementasi operasional.

Ketidakjelasan definisi mengenai ancaman siber, tindak pidana siber, dan insiden siber dalam peraturan perundang-undangan yang ada menyebabkan ambiguitas dalam penentuan jurisdiksi dan kewenangan BIN. Hal ini dapat menyebabkan tumpang tindih kewenangan dengan lembaga lain atau sebaliknya, kekosongan kewenangan dalam kasus tertentu.

Kekosongan operasional operasional yang mengatur prosedur dan mekanisme penanggulangan tindak pidana siber menjadi kelemahan dalam substansi hukum yang serius. Tidak adanya *Standard Operating Procedures* (SOP) yang komprehensif dan detail menyebabkan inkonsistensi dalam pelaksanaan tugas dan potensi pelanggaran prosedur.

Substansi hukum yang ada juga belum mengatur secara memadai aspek perlindungan hak asasi manusia dalam operasi siber BIN. Ketidakjelasan batasan kewenangan pengawasan dan pengumpulan data dapat menimbulkan potensi pelanggaran hak privasi dan hak konstitusional lainnya.

3) Kelemahan dalam Budaya Hukum

Budaya hukum dalam konteks peran BIN menghadapi tantangan dalam adaptasi terhadap kompleksitas permasalahan siber.

Budaya kerahasiaan yang melekat pada institusi intelijen seringkali bertentangan dengan tuntutan transparansi dan akuntabilitas dalam negara demokratis.

Budaya koordinasi antar lembaga masih lemah dan sering diwarnai oleh ego sektoral. Masing-masing lembaga cenderung mempertahankan domain kewenangan masing-masing tanpa mempertimbangkan kebutuhan koordinasi yang optimal dalam menghadapi ancaman siber.

Budaya organisasi dalam BIN yang masih konvensional belum sepenuhnya beradaptasi dengan karakteristik operasi siber yang membutuhkan pendekatan agile dan inovatif. Resistensi terhadap perubahan dari sebagian personel dapat menghambat adopsi teknologi dan metodologi baru.

Budaya hukum masyarakat Indonesia yang masih dalam tahap adaptasi terhadap teknologi digital juga mempengaruhi efektivitas peran BIN. Kurangnya pemahaman masyarakat mengenai ancaman siber dapat menghambat dukungan publik terhadap upaya penanggulangan tindak pidana siber.

b. Kelemahan Aspek Regulasi dan Kepastian Hukum

1) Ketidakjelasan Kewenangan dan Yurisdiksi

Kelemahan mendasar dalam aspek regulasi terletak pada ketidakjelasan kewenangan operasional BIN di domain siber. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memberikan mandat yang bersifat umum tanpa spesifikasi khusus mengenai kewenangan dalam penanganan tindak pidana siber. Ketidakjelasan ini menimbulkan ambiguitas dalam implementasi operasional dan potensi konflik kewenangan dengan lembaga lain.

Permasalahan yang diajukan menjadi semakin kompleks mengingat sifat tindak pidana siber yang seringkali bersifat lintas batas negara. BIN menghadapi kesulitan dalam menentukan batasan kewenangan teritorial dan personal dalam penanganan kasus siber yang melibatkan banyak yurisdiksi..

Ketidakjelasan pembagian peran dan tanggung jawab antara BIN dengan BSSN sebagai lembaga yang memiliki mandat khusus dalam keamanan siber menjadi sumber konflik yuridis. Tidak adanya delineasi yang tegas mengenai domain kewenangan masing-masing lembaga menyebabkan duplikasi usaha dan inefisiensi sumber daya.

Aspek kewenangan BIN dalam melakukan pengawasan dan penyadapan komunikasi dalam konteks siber juga belum diatur secara eksplisit. Ketidakjelasan ini dapat menimbulkan risiko pelanggaran hak konstitusional dan tantangan hukum terhadap operasi yang dilakukan.

2) Kekosongan Regulasi Operasional

BIN menghadapi kekosongan regulasi operasional yang signifikan dalam penanggulangan tindak pidana siber. Tidak adanya peraturan pelaksanaan yang spesifik mengatur standar operasional, prosedur, mekanisme koordinasi, dan protokol penanganan insiden siber menyebabkan ketidakpastian dalam implementasi.

Kekosongan regulasi ini berdampak pada aspek akuntabilitas dan transparansi operasi BIN. Tanpa kerangka hukum yang jelas mengenai batasan kewenangan dan mekanisme pengawasan, terdapat potensi perlindungan kekuasaan dan pelanggaran akibat proses. Tidak adanya regulasi yang mengatur kerjasama antar instansi dalam penanganan kejadian siber menyebabkan koordinasi yang bersifat ad hoc dan tidak terstruktur. Hal ini menghambat efektivitas respons terhadap ancaman siber yang memerlukan tindakan terkoordinasi.

Kekosongan regulasi juga terlihat dalam aspek kerjasama internasional untuk penanganan tindak pidana siber transnasional. BIN tidak memiliki kerangka hukum yang mampu untuk melakukan kerjasama dengan badan intelijen asing dalam berbagi informasi dan respons terkoordinasi.

3) Inkonsistensi Peraturan Perundang-undangan

Sistem peraturan perundang-undangan yang mengatur domain keamanan siber masih mengalami inkonsistensi dan

fragmentasi. Berbagai undang-undang dan peraturan yang terkait dengan keamanan siber tidak sepenuhnya harmonis dan terintegrasi, sehingga menimbulkan kebingungan dalam implementasi.

Inkonsistensi ini terlihat dalam perbedaan terminologi, definisi, dan pendekatan yang digunakan dalam berbagai peraturan. Hal ini menyebabkan penafsiran yang berbeda-beda dalam penerapan hukum dan potensi ketidakpastian hukum. Tidak adanya hirarkhi yang jelas dalam peraturan perundang-undangan terkait keamanan siber juga menimbulkan permasalahan dalam penerapan. Konflik antar peraturan dapat menghambat implementasi yang efektif dan menimbulkan tantangan hukum.

c. Kelemahan Aspek Kelembagaan dan Struktural

1) Fragmentasi Koordinasi Antar Lembaga

Struktur kelembagaan keamanan siber nasional yang tersebar di berbagai institusi menciptakan tantangan koordinasi yang signifikan. BIN, BSSN, Polri, TNI, dan kementerian terkait memiliki mandat yang bersinggungan namun tidak memiliki mekanisme koordinasi yang terintegrasi secara optimal.

Fragmentasi ini diperburuk oleh ego sektoral yang masih kuat di masing-masing lembaga. Setiap institusi cenderung mempertahankan domain kewenangan dan sumber daya tanpa mempertimbangkan kebutuhan sinergi dalam menghadapi ancaman siber yang bersifat multidimensional.

Tidak adanya *lead agency* yang jelas dalam penanganan kejadian siber nasional menyebabkan kebingungan dalam struktur komando dan kendali. Hal ini dapat menghambat pengambilan keputusan cepat yang diperlukan dalam manajemen krisis.

Mekanisme koordinasi yang ada masih bersifat *ad hoc* dan belum terinstitusionalisasi dengan baik. Koordinasi seringkali bergantung pada hubungan pribadi daripada kerangka kelembagaan yang ditetapkan.

2) Keterbatasan Kapasitas Organisasi

BIN menghadapi keterbatasan kapasitas organisasi dalam menghadapi kompleksitas dan volume ancaman siber yang terus meningkat. Struktur organisasi yang masih konvensional belum sepenuhnya beradaptasi dengan karakteristik operasi siber yang membutuhkan fleksibilitas dan *agility*.

Keterbatasan ini tercermin dalam aspek resource allocation yang belum optimal untuk mendukung operasi siber. BIN menghadapi *challenges* dalam mengalokasikan sumber daya manusia, teknologi, dan anggaran untuk mengembangkan kapabilitas siber yang memadai.

Budaya organisasi yang masih hierarkis dan birokratis menghambat penerapan metodologi kerja yang agile dan adaptif. Proses pengambilan keputusan yang panjang dapat mengurangi respons terhadap ancaman siber yang memerlukan tindakan segera.

Peningkatan kapasitas dalam organisasi juga menghadapi tantangan dalam hal manajemen pengetahuan dan pembelajaran kelembagaan. BIN belum memiliki sistem yang efektif untuk menangkap, menyimpan, dan berbagi pengetahuan yang diperlukan untuk perbaikan berkelanjutan.

3) Keterbatasan Struktur Pengawasan

Struktur pengawasan terhadap operasi BIN dalam domain siber masih lemah dan tidak memadai. Tidak adanya badan pengawas khusus yang memiliki keahlian dalam operasi *cyber* menyebabkan kurangnya *checks and balances* dalam sistem. Mekanisme pengawasan internal dalam BIN juga belum sepenuhnya berkembang untuk menghadapi kompleksitas operasi siber. Mekanisme audit internal dan kepatuhan perlu diperkuat untuk memastikan kepatuhan terhadap standar hukum dan etika.

Pengawasan parlemen terhadap BIN dalam domain siber juga menghadapi keterbatasan dalam hal keahlian teknis dan akses terhadap informasi rahasia. Hal ini menghambat efektivitas pengawasan legislatif terhadap operasi siber. Mekanisme pengawasan peradilan untuk kategori tertentu dari operasi siber juga belum dibangun dengan baik. Tidak adanya pengadilan siber khusus atau hakim yang ditunjuk dengan keahlian teknis dapat menghambat peninjauan kembali secara efektif.

d. Kelemahan Aspek Sumber Daya Manusia

1) Defisit Keahlian Teknis

BIN menghadapi kekurangan personel yang memiliki keahlian teknis spesifik dalam bidang keamanan siber. Skill gap ini sangat signifikan mengingat kompleksitas dan evolusi pesat dari teknologi dan ancaman siber. Kurangnya keahlian dalam bidang analisis malware, forensik digital, respons insiden, dan perburuan ancaman cyber menjadi kelemahan kritis.

Gap keahlian ini semakin mengkhawatirkan mengingat perkembangan teknologi yang sangat cepat. BIN kesulitan untuk mengikuti tren teknologi terbaru seperti kecerdasan buatan, komputasi kuantum, dan *blockchain* yang mulai dieksploitasi oleh pelaku kejahatan siber.

Keterbatasan keahlian ini juga tercermin dalam kurangnya pemahaman terhadap ancaman persisten tingkat lanjut dan vektor serangan canggih yang digunakan oleh aktor negara. BIN memerlukan personel dengan keahlian khusus dalam atribusi siber, analisis geopolitik, dan analisis intelijen strategis. Tantangan rekrutmen juga menjadi permasalahan serius dalam mengatasi defisit keahlian. BIN menghadapi persaingan ketat dengan sektor swasta dalam menarik talenta berkualitas tinggi. Kompensasi dan jalur karir yang ditawarkan sektor swasta seringkali lebih menarik dibandingkan sektor pemerintah.

2) Keterbatasan Program Pengembangan Kapasitas

Program pengembangan kapasitas personel BIN dalam bidang keamanan siber masih terbatas baik dari segi kuantitas maupun kualitas. Tidak adanya program pelatihan berkelanjutan yang komprehensif dan terkini menyebabkan kesenjangan keterampilan yang semakin melebar antara kemampuan personel dengan kebutuhan operasional. Program pelatihan yang ada seringkali bersifat ad hoc dan tidak terintegrasi dalam rencana strategis pengembangan sumber daya manusia. BIN belum memiliki kurikulum yang terstruktur untuk mengembangkan keahlian dalam berbagai aspek keamanan siber secara sistematis.

Keterbatasan kesempatan pelatihan internasional juga menghambat pengembangan kapasitas personel. Paparan terhadap praktik terbaik internasional dan teknologi mutakhir sangat penting untuk meningkatkan kapabilitas operasional. Jaminan mutu dalam program pelatihan juga masih lemah. BIN belum memiliki mekanisme penilaian dan sertifikasi yang terstandar untuk memastikan bahwa pelatihan yang diberikan mencapai tujuan pembelajaran yang ditetapkan.

3) Tantangan Retensi Personel

BIN menghadapi tantangan serius dalam retensi talenta, dimana personel yang telah dilatih di bidang keamanan siber seringkali dipindahkan ke sektor swasta yang menawarkan kompensasi yang lebih menarik. Brain drain ini menyebabkan

hilangnya pengetahuan dan kebutuhan institusi untuk terus melakukan perekrutan dan pelatihan personel baru. Peluang pengembangan karir di BIN untuk spesialisasi cyber security juga masih terbatas. Tidak adanya jalur karir yang jelas bagi para profesional keamanan cyber dapat mengurangi motivasi personel untuk mengembangkan keahlian jangka panjang dalam bidang ini.

Keseimbangan kehidupan kerja dalam operasi siber yang seringkali memerlukan *standby* 24/7 juga menjadi faktor yang mempengaruhi tingkat retensi. BIN perlu mengembangkan kebijakan sumber daya manusia yang lebih mendukung terhadap kebutuhan personel keamanan siber. Sistem pengakuan dan penghargaan atas prestasi dalam operasi keamanan siber juga belum memadai. Personel yang memberikan kontribusi signifikan dalam operasi siber perlu mendapatkan pengakuan yang sesuai untuk mempertahankan motivasi dan komitmen.

e. Kelemahan Aspek Teknologi dan Infrastruktur

1) Keterbatasan Infrastruktur Teknologi

BIN mengatasi keterbatasan infrastruktur teknologi yang signifikan dalam mendukung operasi keamanan siber yang efektif. Keterbatasan ini mencakup kurangnya sistem pemantauan dan deteksi yang canggih, keterbatasan kapasitas komputasi untuk menganalisis data besar, dan kurangnya alat dan platform yang

diperlukan untuk intelijen ancaman cyber. Infrastruktur yang ada juga belum terintegrasi penuh dan dapat dioperasikan dengan sistem yang digunakan oleh lembaga lain. Hal ini menghambat pertukaran informasi dan koordinasi operasional dalam penanggulangan tindak pidana siber yang memerlukan respons multi-lembaga.

Standardisasi teknologi yang belum seragam menyebabkan inefisiensi dan potensi kerentanan keamanan. BIN menghadapi tantangan dalam mengintegrasikan berbagai sistem dan platform yang menggunakan standar dan protokol yang berbeda. Skalabilitas dari infrastruktur yang ada juga menjadi permasalahan serius. Dengan meningkatnya volume dan kompleksitas ancaman siber, BIN memerlukan infrastruktur yang dapat berkembang sesuai dengan kebutuhan operasional yang dinamis.

2) Keterlambatan Adopsi Teknologi Terdepan

BIN mengalami keterlambatan dalam menerapkan teknologi terdepan yang diperlukan untuk mengatasi ancaman siber modern. Proses pengadaan teknologi yang panjang dan birokratis menyebabkan kesenjangan antara kebutuhan operasional dengan kemampuan yang tersedia. Proses penilaian dan evaluasi teknologi yang belum efisien juga menghambat penerapan teknologi baru

secara cepat. BIN memerlukan mekanisme yang lebih gesit untuk memancarkan dan mengadopsi teknologi baru yang relevan.

Keterlambatan ini juga disebabkan oleh terbatasnya alokasi anggaran untuk investasi teknologi. BIN menghadapi persaingan prioritas dalam alokasi sumber daya yang terbatas, sehingga investasi teknologi seringkali tidak mendapat prioritas yang memadai.

Resistensi terhadap perubahan dari sebagian personel yang masih nyaman dengan teknologi konvensional juga menghambat adopsi teknologi baru. Manajemen perubahan yang efektif diperlukan untuk memfasilitasi transisi menuju teknologi yang lebih maju.

3) Keamanan dan Keandalan Sistem

Keamanan sistem informasi BIN sendiri menjadi perhatian yang serius mengingat sifat sensitif dari operasi intelijen. BIN menghadapi tantangan dalam keamanan sistem internal dari upaya penetrasi dan sabotase oleh aktor asing atau aktor non-negara.

Sistem redundansi dan backup yang belum memadai juga menjadi kelemahan dalam aspek kelangsungan bisnis. BIN perlu memastikan bahwa operasi kritis dapat terus berlanjut meskipun terjadi kegagalan sistem atau serangan *cyber*.

Prosedur jaminan kualitas dan pengujian untuk sistem yang digunakan dalam operasi siber juga perlu diperkuat. BIN

memerlukan sistem pengujian yang komprehensif untuk memastikan keandalan dan keamanan dari sistem dan aplikasi yang digunakan.

Kemampuan respons insiden untuk keamanan TI internal juga perlu ditingkatkan. BIN harus mampu mendeteksi, merespons, dan memulihkan serangan siber yang menargetkan sistem internal organisasi.

f. Kelemahan Aspek Kerjasama dan Kemitraan

1) Keterbatasan Kerjasama Internasional

BIN menghadapi batasan dalam kerjasama internasional untuk penanggulangan tindak pidana siber yang bersifat transnasional. Tidak adanya kerangka kerja sama yang komprehensif dengan badan intelijen negara lainnya menyebabkan kesulitan dalam melakukan pertukaran informasi dan respons terkoordinasi terhadap ancaman siber lintas negara.

Tantangan diplomatik dalam domain cyber juga kerjasama internasional. Permasalahan terkait kedaulatan, atribusi, dan proporsionalitas dalam operasi siber menjadi hambatan dalam mengembangkan perjanjian kerja sama timbal balik. Hambatan hukum dalam pertukaran informasi dengan badan intelijen asing juga menjadi kendala operasional. BIN menghadapi kendala dalam berbagi intelijen sensitif yang diperlukan untuk kerjasama internasional yang efektif.

Membangun kepercayaan dengan lembaga mitra juga memerlukan waktu yang signifikan. Membangun hubungan dalam komunitas intelijen tidak dapat dilakukan secara instan dan memerlukan konsistensi dalam interaksi profesional.

2) Kurangnya Kemitraan dengan Sektor Swasta

BIN belum mengembangkan kemitraan yang efektif dengan sektor swasta, padahal sebagian besar infrastruktur kritis nasional dikelola oleh entitas swasta. Kurangnya mekanisme kepercayaan dan pertukaran informasi dengan sektor swasta menyebabkan kesenjangan dalam intelijen ancaman dan kesadaran situasional. Perbedaan budaya antara sektor pemerintah dan swasta juga menghambat pengembangan kemitraan yang efektif. Sektor swasta mengutamakan efisiensi dan profitabilitas, sementara lembaga pemerintah mengutamakan keamanan dan kepatuhan.

Hambatan hukum dan peraturan juga meningkatkan pertukaran informasi dengan sektor swasta. Kekhawatiran mengenai tanggung jawab, kerahasiaan, dan kerugian kompetitif menjadi hambatan dalam mengembangkan kemitraan yang bermakna. Program peningkatan kapasitas sektor swasta dalam kesadaran keamanan siber juga masih terbatas. BIN belum mengembangkan program sosialisasi yang komprehensif untuk meningkatkan kesiapan keamanan siber di sektor swasta.

3) Koordinasi dengan Masyarakat Sipil

Keterlibatan organisasi masyarakat sipil dalam pencegahan tindak pidana siber juga masih minim. BIN belum mengembangkan saluran komunikasi yang efektif dengan para akademisi, lembaga think tank, dan kelompok masyarakat sipil yang dapat berkontribusi dalam ekosistem keamanan siber. Kampanye kesadaran masyarakat mengenai ancaman keamanan siber dan upaya pencegahannya juga belum optimal. BIN perlu mengembangkan strategi keterlibatan publik untuk meningkatkan kesadaran keamanan siber di masyarakat.

Transparansi dan akuntabilitas dalam operasi keamanan siber juga menjadi perhatian masyarakat sipil. BIN perlu menemukan keseimbangan antara kebutuhan keamanan operasional dengan tuntutan transparansi yang lebih besar. Inisiatif keamanan siber berbasis komunitas juga belum berkembang dengan baik. BIN dapat berperan dalam memfasilitasi program kesadaran keamanan siber dan peningkatan kapasitas di tingkat masyarakat.

3. Peran BIN dalam Penanggulangan Tindak Pidana Siber Berbasis Kepastian Hukum

a. Konseptualisasi Kepastian Hukum dalam Konteks Keamanan Siber Berdasarkan Teori Gustav Radbruch

1) Landasan Teoritis Kepastian Hukum Gustav Radbruch

Dalam menganalisis peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum, penulis menggunakan

kerangka teoritis kepastian hukum yang dikembangkan oleh Gustav Radbruch. Menurut Radbruch, kepastian hukum merupakan salah satu dari tiga nilai dasar hukum (*rechtswerte*) bersama dengan keadilan (*gerechtigkeit*) dan kegunaan (*zweckmäßigkeit*).

Radbruch menekankan bahwa kepastian hukum tidak hanya berkaitan dengan prediktabilitas dalam penerapan hukum, tetapi juga mencakup aspek legitimasi dan konsistensi dalam sistem hukum. Dalam konteks penanggulangan tindak pidana siber, kepastian hukum menjadi landasan yang penting untuk memastikan bahwa tindakan BIN memiliki dasar hukum yang jelas dan dapat dipertanggungjawabkan.

Teori Radbruch juga mengakui adanya ketegangan antara kepastian hukum dengan nilai-nilai hukum lainnya. Dalam keadaan tertentu, kepastian hukum dapat berkonflik dengan keadilan substantif atau kegunaan praktisnya. Namun, Radbruch menekankan pentingnya mencari keseimbangan antara nilai ketiga tersebut dalam sistem hukum yang ideal.

Dalam penerapannya pada domain siber, teori Radbruch memberikan kerangka untuk menganalisis bagaimana kepastian hukum dapat diwujudkan tanpa mengorbankan efektivitas operasional BIN dalam menghadapi ancaman siber yang dinamis dan berkembang.

2) Dimensi Kepastian Hukum dalam Operasi Siber BIN

Kepastian hukum dalam pencegahan tindak pidana siber oleh BIN meliputi tiga dimensi utama berdasarkan kerangka Radbruch. Pertama, norma kepastian (*normative surety*) yang mengacu pada kejelasan peraturan perundang-undangan yang mengatur kewenangan dan batasan operasional BIN dalam domain siber.

Kedua, kepastian implementasi (kepastian pelaksanaan) yang berkaitan dengan standarisasi prosedur dan cara operasional. Dimensi ini memastikan bahwa setiap personel BIN memahami dengan jelas prosedur yang harus diikuti dalam menjalankan operasi siber.

Ketiga, kepastian penegakan (*enforcement surety*) yang mencakup konsistensi dalam penerapan sanksi dan tindakan akuntabilitas. Dimensi ini memastikan bahwa pelanggaran terhadap persyaratan hukum dan prosedur akan mendapat konsekuensi yang sesuai dan konsisten.

Dimensi ketiga kepastian hukum ini harus terintegrasi dalam kerangka hukum komprehensif yang mengatur peran BIN dalam tindakan pidana siber. Integrasi ini diperlukan untuk menciptakan sistem yang koheren dan efektif.

3) Prinsip-Prinsip Kepastian Hukum dalam Konteks Siber

Kepastian implementasi hukum dalam operasi siber BIN harus didasarkan pada prinsip-prinsip fundamental *rule of law*. Prinsip legalitas menetapkan bahwa setiap tindakan BIN harus

memiliki dasar hukum yang jelas dan spesifik. Dalam domain siber, hal ini berarti bahwa aktivitas pengawasan, pengumpulan data, dan operasi siber harus diotorisasi oleh ketentuan hukum yang tegas.

Prinsip proporsionalitas memastikan bahwa tindakan yang diambil BIN sebanding dengan ancaman yang dihadapi. Dalam konteks keamanan siber, prinsip ini mengatur bahwa tindakan intrusif hanya dapat dilakukan jika dibenarkan berdasarkan tingkat keparahan ancaman dan tidak ada tindakan alternatif yang tidak terlalu mengganggu.

Prinsip akuntabilitas menetapkan bahwa BIN harus bertanggung jawab atas tindakan yang dilakukan dalam operasi siber. Hal ini mencakup kewajiban untuk melaporkan kepada pihak yang berwenang dan menyerahkan kepada mekanisme pengawasan yang telah ditetapkan.

Prinsip transparansi, meskipun dibatasi oleh kebutuhan keamanan operasional, tetap menjadi elemen penting dalam kepastian hukum. BIN harus memberikan informasi yang memadai kepada badan pengawas dan masyarakat mengenai kerangka umum operasi keamanan siber.

b. Kerangka Regulasi untuk Kepastian Hukum Operasi BIN

1) Reformulasi Kewenangan yang Spesifik dan Tegas

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan reformulasi komprehemsif

terhadap *legal framework* yang mengatur kewenangan BIN. Hal ini dapat diwujudkan melalui amandemen Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara atau penerbitan undang-undang khusus tentang keamanan siber nasional.

Reformulasi ini harus mencakup definisi yang jelas dan komprehensif mengenai ancaman siber, insiden siber, dan kejahatan siber yang menjadi jurisdiksi BIN. Definisi ini harus cukup spesifik untuk memberikan panduan yang jelas namun cukup fleksibel untuk mengakomodasi perubahan alam dari ancaman dunia. Kerangka hukum baru juga harus mengatur mekanisme pembagian kewenangan antara BIN dengan lembaga lain seperti BSSN, Polri, dan TNI. Penggambaran ini harus didasarkan pada spesialisasi fungsional dan keunggulan komparatif masing-masing lembaga dalam menghadapi berbagai jenis ancaman siber.

Aspek kerjasama internasional juga harus diatur secara eksplisit dalam kerangka hukum yang baru. BIN memerlukan kewenangan hukum yang jelas untuk terlibat dalam pertukaran informasi dan operasi gabungan dengan badan intelijen asing dalam memerangi ancaman siber transnasional.

2) Pengembangan Standar Operasional Prosedur yang Komprehensif

Kepastian hukum dalam operasi BIN memerlukan pengembangan *Standard Operating Procedures* (SOP) yang

komprehensif dan rinci. SOP ini harus mengatur seluruh aspek operasi keamanan siber mulai dari deteksi ancaman, analisis, respons, hingga prosedur pemulihan. SOP harus mencakup pedoman yang jelas untuk pengambilan keputusan dalam berbagai skenario. Pohon keputusan dan prosedur eskalasi harus ditetapkan untuk memastikan bahwa personel dapat membuat keputusan yang tepat dalam situasi yang sensitif terhadap waktu tanpa melanggar persyaratan hukum.

Aspek perlindungan hak asasi manusia dan perlindungan privasi harus terintegrasi dalam setiap tahapan prosedur operasional. SOP harus mencakup ketentuan khusus untuk melindungi hak konstitusional dan meminimalkan dampak tambahan terhadap individu yang bukan sasaran. Mekanisme kendali mutu dan pemantauan kepatuhan juga harus dimasukkan dalam SOP. Audit dan penilaian rutin harus dilakukan untuk memastikan kepatuhan terhadap prosedur yang ditetapkan dan mengidentifikasi area yang perlu ditingkatkan.

3) Mekanisme Pengawasan dan Akuntabilitas

Kerangka kepastian hukum harus mencakup mekanisme pengawasan dan akuntabilitas yang kuat untuk memastikan bahwa BIN beroperasi dalam batas-batas hukum. Sistem pengawasan berlapis harus dibangun yang mencakup pengawasan internal, pengawasan eksekutif, pengawasan legislatif, dan pengawasan

yudikatif. Mekanisme pengawasan internal harus mencakup inspektur jenderal atau ombudsman independen yang memiliki wewenang untuk menyelidiki pengaduan dan melakukan audit kepatuhan. Badan pengawas internal ini harus memiliki akses terhadap semua informasi dan wewenang yang relevan untuk membuat rekomendasi yang mengikat.

Pengawasan legislatif harus dilakukan oleh komite khusus parlemen yang memiliki izin keamanan dan keahlian teknis untuk melakukan pengawasan yang efektif terhadap operasi siber. Komite ini harus memiliki jadwal pengarahan rutin dan wewenang untuk melakukan investigasi. Mekanisme pengawasan yudisial harus dibentuk untuk kategori operasi siber tertentu yang melibatkan pengawasan intrusif atau pengumpulan data. Pengadilan siber khusus atau hakim yang ditunjuk dengan keahlian teknis dapat memberikan peninjauan kembali secara efektif.

c. *Framework* Koordinasi Berbasis Kepastian Hukum

1) Mekanisme Koordinasi Kelembagaan

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan mekanisme koordinasi kelembagaan yang diatur secara legal dan formal. Mekanisme ini dapat berupa pembentukan *National Cyber Security Coordinate Center* (NCSCC) yang memiliki mandat hukum yang jelas. NCSCC harus dipimpin oleh pejabat tingkat tinggi dengan keanggotaan dari

BIN, BSSN, Polri, TNI, dan kementerian terkait. Struktur dan wewenang NCSCC harus diatur dalam instrumen hukum yang spesifik untuk memastikan legitimasi dan efektivitas.

Kerangka hukum harus mengatur peran dan tanggung jawab yang jelas untuk masing-masing anggota dalam NCSCC. Penggambaran fungsi harus didasarkan pada keunggulan komparatif dan kompetensi inti masing-masing lembaga. Prosedur pengambilan keputusan dalam NCSCC juga harus diatur secara rinci dalam kerangka hukum. Mekanisme pembangunan konsensus, prosedur pemungutan suara, dan mekanisme pengikatan harus dibentuk untuk memfasilitasi pengambilan keputusan yang efektif.

2) *Framework* Berbagi Informasi

Kepastian hukum dalam pertukaran informasi antar lembaga memerlukan kerangka hukum komprehensif yang mengatur klasifikasi informasi, prosedur deklasifikasi, protokol berbagi, dan perlindungan informasi sensitif. *Framework* ini harus menyeimbangkan antara kebutuhan operasional dengan persyaratan keamanan. Kerangka hukum harus mencakup perlindungan tanggung jawab bagi personel dan lembaga yang terlibat dalam pertukaran informasi dengan itikad baik. Klausul ganti rugi harus memberikan perlindungan yang memadai untuk mendorong keterbukaan dalam pembagian intelijen ancaman.

Perlindungan data dan perlindungan privasi juga harus dimasukkan dalam kerangka berbagi informasi. Prosedur untuk menangani data pribadi yang dikumpulkan secara tidak sengaja harus ditetapkan untuk memastikan kepatuhan terhadap hak privasi. Pertukaran informasi internasional juga harus diatur dalam kerangka hukum dengan perlindungan yang tepat untuk melindungi informasi keamanan nasional. Perjanjian timbal balik dengan lembaga asing harus mempunyai dasar hukum yang memadai.

3) Mekanisme Respons Terintegrasi

Kerangka hukum harus mengatur mekanisme respons terpadu terhadap insiden siber besar yang memerlukan koordinasi multi-lembaga. Struktur komando dan kendali yang jelas harus dibentuk untuk memfasilitasi respons yang cepat dan efektif. Sistem klasifikasi insiden harus dikembangkan untuk menentukan tingkat respons yang tepat dan keterlibatan lembaga. Kriteria klasifikasi harus obyektif dan terukur untuk memastikan penerapan yang konsisten.

Mekanisme alokasi sumber daya harus diatur dalam kerangka hukum untuk memastikan pembagian biaya dan sumber daya yang adil dalam operasi bersama. Formula pembagian beban harus transparan dan adil. Prosedur peninjauan pasca-insiden juga harus ditetapkan untuk memfasilitasi pembelajaran dan perbaikan. Laporan pasca tindakan harus diperlukan untuk semua insiden besar

dengan rekomendasi untuk meningkatkan kemampuan respons di masa depan.

d. Perlindungan Hak Asasi dan Kebebasan Sipil

1) *Framework* Perlindungan Privasi

Peran BIN dalam penanggulangan tindak pidana siber harus menerapkan kerangka perlindungan privasi yang kuat yang sesuai dengan jaminan konstitusi dan standar hak asasi manusia internasional. Kerangka kerja ini harus mengatur batasan pengumpulan data, periode penyimpanan, batasan pembagian, dan persyaratan pemberitahuan. Penilaian dampak privasi harus diperlukan untuk semua operasi keamanan siber yang melibatkan pengumpulan atau pemrosesan data pribadi. Penilaian ini harus dilakukan sebelum implementasi program atau teknologi baru.

Prinsip minimalisasi data harus diterapkan dalam semua aktivitas pengumpulan. BIN harus mengumpulkan hanya data yang diperlukan untuk tujuan keamanan yang sah dan menghindari pengumpulan data yang berlebihan atau sembarangan. Mekanisme hak-hak individu harus dibentuk untuk memungkinkan warga negara mengakses informasi tentang data yang dikumpulkan dan pengumpulan atau pemrosesan yang melanggar hukum. Hak untuk mendapatkan pemulihan harus diberikan kepada individu yang terkena dampak pengawasan yang salah.

2) *Safeguards* Proses Hukum yang Adil

Karena proses pengamanan harus tertanam dalam setiap aktivitas operasional BIN dalam domain siber. Perlindungan prosedural harus mencakup hak untuk memberi tahu (dengan pengecualian untuk operasi yang sedang berlangsung), hak untuk menentang perintah pengawasan, dan hak untuk mendapatkan perwakilan hukum. Persyaratan surat perintah harus ditetapkan untuk kategori tertentu dari operasi cyber yang mengganggu. Otorisasi yudisial harus diperlukan untuk operasi yang melibatkan gangguan privasi yang signifikan atau pembatasan hak konstitusional.

Mekanisme banding harus tersedia bagi individu yang yakin bahwa hak mereka telah dilanggar dalam operasi keamanan siber. Badan peninjau independen harus dibentuk untuk menangani pengaduan dan memberikan solusi. Mekanisme kompensasi harus disediakan untuk kerusakan yang disebabkan oleh operasi cyber yang salah. Korban harus memiliki akses terhadap pemulihan yang memadai termasuk kompensasi moneter dan tindakan korektif.

3) Transparensi dan Akuntabilitas Publik

Meskipun pertimbangan keamanan operasional membatasi transparansi penuh, BIN harus menyediakan informasi publik yang memadai tentang kerangka umum dan kebijakan operasi keamanan siber. Laporan publik tahunan harus diterbitkan dengan redaksi yang sesuai. Mekanisme konsultasi publik harus dibentuk untuk

perubahan kebijakan besar yang berdampak pada kebebasan sipil. Keterlibatan pemangku kepentingan harus difasilitasi melalui forum dan saluran yang sesuai.

Kebijakan hubungan media harus dikembangkan untuk memberikan informasi yang tepat kepada publik tentang ancaman keamanan siber dan tanggapan pemerintah tanpa mengorbankan keamanan operasional. Program penjangkauan pendidikan harus dilakukan untuk meningkatkan pemahaman masyarakat tentang ancaman keamanan siber dan upaya perlindungan individu. Kampanye kesadaran masyarakat dapat membantu menciptakan masyarakat yang terinformasi.

e. *Framework* Kerjasama Internasional

1) Perjanjian Bilateral dan Multilateral

Peran BIN dalam penanggulangan tindak pidana siber berbasis kepastian hukum memerlukan kerangka hukum internasional yang komprehensif. Perjanjian bilateral dengan negara-negara mitra utama harus dibuat untuk memfasilitasi pertukaran informasi dan operasi bersama. Kerangka kerja multilateral seperti partisipasi dalam organisasi dan inisiatif keamanan siber internasional harus memiliki dasar hukum dalam hukum domestik. Proses ratifikasi oleh parlemen harus diikuti untuk menjamin legitimasi demokratis.

Kerangka hukum harus mengatasi masalah yurisdiksi dalam investigasi siber lintas batas. Perjanjian bantuan hukum timbal balik harus diperbarui agar mencakup kejahatan dunia maya dan bukti digital secara memadai. Pengaturan ekstradisi terhadap penjahat dunia maya harus diperkuat melalui instrumen hukum yang sesuai. Perjanjian ekstradisi tradisional mungkin perlu diperbarui untuk mencakup kategori kejahatan dunia maya yang terus berkembang.

2) Standardisasi Hukum Internasional

BIN harus berpartisipasi aktif dalam upaya internasional untuk mengembangkan standar umum dan praktik terbaik dalam penegakan hukum keamanan siber. Harmonisasi peraturan perundang-undangan dalam negeri dengan standar internasional harus diupayakan. Kerangka hukum internasional seperti Konvensi Budapest tentang Kejahatan Dunia Maya harus dipertimbangkan untuk diadopsi dengan adaptasi yang tepat untuk sistem hukum domestik. Manfaat dan tantangan dari instrumen internasional harus dievaluasi secara cermat.

Program peningkatan kapasitas di negara-negara berkembang dapat membantu menciptakan pendekatan bersama untuk penegakan hukum keamanan siber. Program bantuan teknis dapat memperkuat kemampuan keamanan siber regional.

Keterlibatan diplomatik dalam forum internasional harus didukung dengan kerangka hukum yang memadai. Insan BIN yang terlibat dalam kerja sama internasional harus mempunyai wewenang dan arahan yang jelas.

3) Penyelesaian Sengketa Internasional

Kerangka hukum harus membahas mekanisme penyelesaian sengketa untuk kerja sama keamanan siber internasional. Prosedur untuk menyelesaikan konflik atau perselisihan dengan mitra asing harus ditetapkan. Tantangan atribusi dalam insiden siber internasional memerlukan kerangka hukum khusus. Prosedur untuk menentukan tanggung jawab dan tanggapan yang tepat harus dikembangkan melalui konsultasi dengan mitra internasional.

Masalah kekebalan diplomatik terhadap personel BIN yang beroperasi di luar negeri harus ditangani dalam kerangka hukum. Status perjanjian dengan negara tuan rumah harus memberikan perlindungan yang memadai. Mekanisme arbitrase internasional dapat digunakan untuk menyelesaikan sengketa keamanan siber internasional yang kompleks. Kerangka hukum harus memberikan kewenangan untuk berpartisipasi dalam mekanisme tersebut.

f. Pengembangan Kapasitas dan Profesionalisme

1) Program Pendidikan dan Pelatihan Hukum

Peran BIN berbasis kepastian hukum memerlukan program pelatihan hukum yang komprehensif untuk personel yang terlibat

dalam operasi siber. Pelatihan harus mencakup hukum konstitusi, hukum acara pidana, hukum internasional, hukum hak asasi manusia, dan hukum siber. Program pendidikan hukum harus mencakup studi kasus praktis dan latihan berbasis skenario yang mencerminkan tantangan operasional dunia nyata. Latihan simulasi dapat membantu personel memahami implikasi hukum dari keputusan operasional.

Persyaratan pendidikan hukum yang berkelanjutan harus ditetapkan untuk memastikan bahwa personel selalu mengikuti perkembangan hukum dalam hukum siber. Pelatihan penyegaran secara berkala harus diwajibkan bagi seluruh personel operasional. Kemitraan dengan fakultas hukum dan organisasi profesi hukum dapat meningkatkan kualitas program pelatihan hukum. Keahlian eksternal dapat memberikan perspektif yang berharga mengenai permasalahan hukum.

2) Sertifikasi dan Standar Profesional

BIN perlu mengembangkan program sertifikasi profesi yang mencakup kompetensi hukum sebagai persyaratan inti. Standar sertifikasi harus komprehensif dan diperbarui secara berkala untuk mencerminkan lanskap hukum yang terus berkembang. Kode etik personel keamanan siber BIN harus ditetapkan dengan pedoman yang jelas untuk berperilaku profesional. Standar etika harus mengatasi tantangan unik dalam operasi keamanan siber.

Prosedur disiplin untuk pelanggaran standar hukum atau etika harus ditetapkan. Perlindungan proses yang semestinya harus diberikan dalam proses disipliner sambil menjaga disiplin organisasi. Sistem evaluasi kinerja harus memasukkan kepatuhan hukum sebagai indikator kinerja utama. Personil yang menunjukkan keunggulan dalam kepatuhan hukum harus menerima pengakuan yang sesuai.

3) Penelitian dan Pengembangan Hukum

BIN harus membangun kemampuan penelitian hukum agar tetap mengikuti perkembangan hukum siber. Kemitraan penelitian dengan institusi akademis dapat meningkatkan kemampuan analitis. Pengembangan doktrin hukum untuk operasi keamanan siber harus dilakukan secara berkelanjutan. Praktik terbaik dan pembelajaran harus didokumentasikan dan dibagikan kepada pemangku kepentingan terkait.

Studi hukum komparatif internasional dapat memberikan wawasan untuk memperbaiki kerangka hukum dalam negeri. Pembelajaran dari pengalaman negara lain dapat menjadi masukan bagi pengembangan kebijakan. Program publikasi untuk berbagi temuan penelitian dengan komunitas profesional yang lebih luas dapat memberikan kontribusi terhadap pembangunan secara

keseluruhan di lapangan. Kontribusi akademis dapat meningkatkan reputasi BIN sebagai thought leader.

g. Tata Kelola Teknologi dan Kepatuhan Hukum

1) *Framework* Akuisisi Teknologi

Peran BIN dalam domain siber memerlukan kerangka hukum yang komprehensif untuk akuisisi teknologi yang memastikan kepatuhan terhadap persyaratan hukum dan standar etika. Prosedur pengadaan harus memasukkan tinjauan hukum sebagai persyaratan wajib. Kriteria penilaian teknologi harus memasukkan faktor kepatuhan hukum sebagai pertimbangan utama. Proses evaluasi vendor harus memeriksa rekam jejak hukum dan kemampuan kepatuhan.

Persyaratan keamanan rantai pasokan harus memperhatikan aspek kepatuhan hukum. Vendor harus menunjukkan kepatuhan terhadap hukum dan peraturan yang berlaku dalam rantai pasokan mereka. Ketentuan kontrak dengan vendor teknologi harus mencakup perlindungan hukum dan persyaratan kepatuhan yang sesuai. Perjanjian vendor harus menetapkan kewajiban hukum dan upaya hukum atas ketidakpatuhan.

2) Manajemen dan Tata Kelola Data

Kerangka hukum tata kelola data dalam operasi siber BIN harus komprehensif dan rinci. Sistem klasifikasi data harus selaras dengan persyaratan hukum untuk perlindungan informasi.

Mekanisme kontrol akses harus menerapkan prinsip-prinsip yang perlu diketahui dan hak istimewa terendah sesuai dengan persyaratan hukum. Prosedur otorisasi harus didokumentasikan dan dapat diaudit.

Kebijakan penyimpanan data harus mematuhi persyaratan hukum sekaligus mendukung kebutuhan operasional. Periode penyimpanan harus ditetapkan berdasarkan kewajiban hukum dan persyaratan operasional. Kebijakan transfer data lintas batas harus memperhatikan batasan dan persyaratan hukum yang berlaku. Perjanjian berbagi data internasional harus memiliki perlindungan hukum yang memadai.

***3)* Audit dan Kepatuhan**

Audit kepatuhan rutin harus dilakukan untuk memastikan kepatuhan terhadap persyaratan hukum dalam operasi teknologi. Cakupan audit harus komprehensif dan mencakup semua kewajiban hukum yang relevan. Pengawasan independen dari operasi teknologi harus dibentuk untuk memberikan penilaian objektif atas kepatuhan hukum. Auditor eksternal dengan izin keamanan yang sesuai dapat memberikan perspektif yang berharga.

Prosedur remediasi terhadap pelanggaran kepatuhan harus ditetapkan. Rencana tindakan perbaikan harus dikembangkan dan diimplementasikan untuk mengatasi kekurangan yang teridentifikasi. Mekanisme pelaporan untuk masalah kepatuhan

harus memfasilitasi identifikasi dan penyelesaian masalah secara cepat. Perlindungan pelapor harus diberikan kepada personel yang melaporkan pelanggaran hukum.

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan analisis komprehensif yang telah dilakukan dengan menggunakan kerangka teoritis Sistem Hukum Lawrence M. Friedman, Teori Kewenangan, dan Teori Kepastian Hukum Gustav Radbruch, dapat disimpulkan bahwa peran BIN dalam penanggulangan tindak pidana siber saat ini masih menghadapi berbagai tantangan fundamental yang memerlukan reformasi sistemik.

Dari perspektif struktur hukum, BIN memiliki landasan hukum yang mendasar namun tidak spesifik untuk domain siber. Substansi hukum yang mengatur peran BIN belum komprehensif dan mengandung berbagai batasan regulasi. Budaya hukum dalam implementasi masih dalam tahap adaptasi terhadap kompleksitas persoalan siber.

Kerangka kepastian hukum yang diusulkan berdasarkan teori Gustav Radbruch menawarkan solusi komprehensif untuk mengatasi kelemahan yang ada. Implementasi dari kerangka ini memerlukan kemauan politik yang kuat, alokasi sumber daya yang memadai, dan komitmen jangka panjang dari seluruh pemangku kepentingan yang terlibat. Dengan diterapkannya kerangka kepastian hukum yang komprehensif, peran BIN dalam penanggulangan tindak pidana siber dapat menjadi lebih efektif, akuntabel, dan berkelanjutan dalam menghadapi ancaman siber yang terus berkembang.

Badan Intelijen Negara (BIN) berperan sebagai garda terdepan dalam mendeteksi, mencegah, dan menangani ancaman siber melalui kegiatan intelijen

siber. Peran ini diwujudkan melalui pengumpulan dan analisis data, pemetaan potensi serangan, pengamanan infrastruktur strategis, serta koordinasi dengan lembaga terkait seperti BSSN, Polri, dan Kemenkominfo. BIN juga melakukan operasi kontra-intelijen siber untuk mencegah infiltrasi pihak asing dan kelompok kriminal siber yang mengancam keamanan nasional.

Badan Intelijen Negara (BIN) menghadapi beberapa kelemahan, antara lain:

1. Regulasi yang belum spesifik terkait kewenangan BIN dalam domain siber, sehingga terjadi tumpang tindih dengan lembaga lain.
2. Keterbatasan SDM dan teknologi dalam menghadapi serangan siber yang semakin kompleks.
3. Minimnya transparansi dan akuntabilitas dalam pelaksanaan tugas siber, yang berpotensi menimbulkan konflik kewenangan.
4. Koordinasi antarlembaga yang belum optimal, menyebabkan respons terhadap ancaman siber sering lambat.

Untuk menjamin kepastian hukum, peran BIN harus dilandasi oleh regulasi yang jelas mengenai batas kewenangan, prosedur pengumpulan data, serta mekanisme kerja sama dengan aparat penegak hukum. Kepastian hukum ini diperlukan agar tindakan BIN tidak menimbulkan pelanggaran hak asasi atau konflik yurisdiksi. BIN juga harus mematuhi prinsip legalitas, proporsionalitas, dan akuntabilitas dalam setiap operasi sibernya agar sejalan dengan hukum positif Indonesia.

B. Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diuraikan, maka penulis memberikan beberapa saran yang diharapkan dapat menjadi bahan pertimbangan dalam upaya peningkatan peran Badan Intelijen Negara (BIN) dalam penanggulangan tindak pidana siber berbasis kepastian hokum, yaitu:

1. Pemerintah perlu memperjelas kewenangan BIN dalam penanggulangan tindak pidana siber melalui revisi UU Intelijen Negara dan regulasi turunan yang mengatur tata cara pengumpulan data, koordinasi, serta pembagian tugas antarinstansi.
2. BIN harus mengembangkan kompetensi SDM siber melalui pelatihan berkelanjutan dan pemanfaatan teknologi mutakhir, termasuk kecerdasan buatan (AI) untuk mendeteksi dan menganalisis ancaman siber secara real-time.
3. Diperlukan mekanisme koordinasi yang lebih solid antara BIN, BSSN, Polri, dan Kemenkominfo agar tidak terjadi tumpang tindih kewenangan dan agar respons terhadap ancaman siber lebih cepat dan terintegrasi.
4. Setiap langkah BIN dalam penanggulangan tindak pidana siber harus sesuai dengan prinsip hukum yang berlaku untuk mencegah pelanggaran hak privasi dan menjamin keadilan hukum.

DAFTAR PUSTAKA

Buku

A.S.S. Tambunan. *Intelijen: Teori, Aplikasi dan Modernisasi*. Jakarta: Pustaka Sinar Harapan, 2018.

Adrian Sutedi. *Hukum Perizinan dalam Sektor Pelayanan Publik*. Jakarta: Sinar Grafika, 2021.

Aharon Barak. *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press, 2012.

Alan Gewirth, *Reason and Morality*, Chicago: University of Chicago Press, 1978

Alasdair MacIntyre, *After Virtue, 3rd Edition*, Notre Dame: University of Notre Dame Press, 2007

Allen W. Wood, *Kant's Ethical Thought*, Cambridge: Cambridge University Press, 1999

Amartya Sen, *Development as Freedom*, New York: Knopf, 1999

Andi Hamzah. *Aspek-aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika, 2017.

Andrews Reath, *Agency and Autonomy in Kant's Moral Theory*, Oxford: Oxford University Press, 2006

Arthur Kaufmann. *Gustav Radbruch: Rechtsdenker, Philosoph, Sozialdemokrat*. München: Piper, 1987.

Badan Intelijen Negara, *Analisis Efektivitas Pertukaran Informasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Analisis Implementasi Tinjauan Yudisial Dalam Operasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Analisis Kasus Operasi Siber Lintas Negara 2022–2024, Laporan Internal,* Jakarta, BIN, 2024

----------, *Analisis Kerja Sama Internasional Keamanan Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Analisis Operasional Siber, Laporan Internal*, Jakarta, BIN, 2025

----------, *Analisis Program Pelatihan Dan Anggaran Keamanan Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Analisis Siklus Pengadaan Teknologi Operasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Analisis Waktu Respons Dan Deteksi Insiden Siber 2024, Laporan Internal,* Jakarta, BIN, 2024

----------, *Audit Pengadaan Teknologi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Audit Prosedur Operasional Siber 2024*, Laporan Internal, Jakarta, BIN, 2024

----------, *Audit Sumber Daya Manusia Operasi Siber 2024, Laporan Internal,* Jakarta, BIN, 2024

----------, *Audit Tata Kelola Data Operasional Siber 2024, Laporan Internal,* Jakarta, BIN, 2024

----------, *Catatan Internal Tim Analisis Intelijen Siber*, Jakarta, BIN, 2025

----------, *Catatan Koordinasi Antar-Lembaga Bidang Siber*, *Dokumen Internal*, Jakarta, BIN, 2025

----------, *Evaluasi Kemampuan Operasional Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Evaluasi Kerjasama Internasional Dalam Keamanan Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Evaluasi Kompetensi Hukum Personel Operasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Evaluasi Struktur Organisasi Dan Efektivitas Operasional 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Evaluasi Transparansi Dan Pemberitahuan Dalam Operasi Pengawasan Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Inventarisasi Infrastruktur Teknologi Operasi Siber 2024, Laporan Internal*, Jakarta: BIN, 2024

----------, *Laporan Analisis Ancaman Siber 2020–2024*, Dokumen Internal, Jakarta, BIN, 2024

----------, *Laporan Benchmarking Program Sertifikasi Profesional Dalam Operasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Laporan Evaluasi Sistem Deteksi Dini Pusat Komando Operasi Siber, Dokumen Internal*, Jakarta, BIN, 2025

----------, *Laporan Kinerja Intelijen Siber Tahun 2024*, Jakarta, BIN, 2025

----------, *Studi Perbandingan Kerangka Hukum Operasi Intelijen Siber 2024, Laporan Internal*, Jakarta: BIN, 2024

----------, *Survei Dan Simulasi Koordinasi Keamanan Siber Nasional 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Survei Kolaborasi Keamanan Siber Dengan Sektor Swasta 2024, Laporan Internal*, Jakarta, BIN, 2024

----------, *Survei Persepsi Publik Tentang Perlindungan Privasi Dalam Operasi Siber 2024, Laporan Internal*, Jakarta, BIN, 2024

Badan Siber dan Sandi Negara, *Laporan Tahunan Pemantauan Keamanan Siber 2021,* Jakarta, BSSN, 2022

----------. *Laporan Tahunan Monitoring Keamanan Siber 2021*. Jakarta, BSSN, 2022.

Bagir Manan. *Teori dan Politik Konstitusi*. Yogyakarta: FH UII Press, 2019.

Bambang Sunggono. *Metodologi Penelitian Hukum*, Cetakan Kesembilan. Jakarta: Raja Grafindo Persada, 2020.

Barbara Herman, *The Practice of Moral Judgment*, Cambridge: Harvard University Press, 1993

Barda Nawawi Arief. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2014.

----------. *Cybercrime dan Cyberlaw*. Semarang: Pustaka Magister, 2015.

Brian Barry, *Justice as Impartiality*, Oxford: Oxford University Press, 1995

Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers, 2020.

Charles R. Beitz, *Political Theory and International Relations, Revised Edition*, Princeton: Princeton University Press, 1999

Christine M. Korsgaard, *Creating the Kingdom of Ends*, Cambridge: Cambridge University Press, 1996

Christopher Bronk and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco". *Survival*, Vol. 55, No. 2, 2013.

Danrivanto Budhijanto. *Cyberlaw dan Revolusi Digital*. Bandung: Logoz Publishing, 2022.

David Miller, *Principles of Social Justice*, Cambridge: Harvard University Press, 1999

Derek Parfit, *Reasons and Persons*, Oxford: Oxford University Press, 1984

Edmon Makarim. *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada, 2019.

Frances M. Kamm, *Intricate Ethics*, New York: Oxford University Press, 2007

Franz Magnis-Suseno. *Etika Politik: Prinsip-prinsip Moral Dasar Kenegaraan Modern*, Edisi Kelima. Jakarta: Gramedia Pustaka Utama, 2021.

G.A. Cohen, *If You're an Egalitarian, How Come You're So Rich?,* Cambridge: Harvard University Press, 2000

Gustav Radbruch. *Legal Philosophy, translated by Kurt Wilk*. Cambridge: Harvard University Press, 1950.

----------. *Rechtsphilosophie*, 8. Auflage. Stuttgart: Koehler Verlag, 1973.

H.L.A. Hart, *The Concept of Law, 3rd Edition,* Oxford: Oxford University Press, 2012

Hans Kelsen, *Pure Theory of Law, translated by Max Knight*, Berkeley: University of California Press, 1967.

Indroharto. *Usaha Memahami Undang-undang tentang Peradilan Tata Usaha Negara*, Cetakan Kelima. Jakarta: Pustaka Sinar Harapan, 2019.

Isaiah Berlin, *Two Concepts of Liberty*, Oxford: Oxford University Press, 1969

Jeffrey Carr. *Inside Cyber Warfare*, 2nd Edition. Sebastopol: O'Reilly Media, 2012.

Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation*, Oxford: Oxford University Press, 1996

Jimly Asshiddiqie. *Hukum Tata Negara dan Pilar-pilar Demokrasi*, Cetakan Kedua. Jakarta: Sinar Grafika, 2018.

----------. *Konstitusi dan Konstitusionalisme Indonesia*, Edisi Revisi. Jakarta: Sinar Grafika, 2021.

Joel Feinberg, *Harm to Others*, New York: Oxford University Press, 1984

John Finnis, *Natural Law and Natural Rights, 2nd Edition*, Oxford: Oxford University Press, 2011

John Rawls, *A Theory of Justice, Revised Edition*, Cambridge: Harvard University Press, 1999

John Stuart Mill, *On Liberty*, London: Penguin Classics, 2006

Johnny Ibrahim. *Teori dan Metodologi Penelitian Hukum Normatif*, Cetakan Ketiga. Malang: Bayumedia Publishing, 2019.

Jonaedi Efendi dan Johnny Ibrahim. *Metode Penelitian Hukum*, Cetakan Kedua. Jakarta: Kencana, 2020.

Joseph Raz, *The Authority of Law, 2nd Edition*, Oxford: Oxford University Press, 2009

Joseph S. Nye Jr. *Cyber Power*. Cambridge: Harvard University Press, 2011.

Josua Sitompul. *Akses Bukti Elektronik Lintas Batas Negara: Memperkuat Hukum dan Praktik Indonesia dalam Penyidikan Tindak Pidana Siber*. Jakarta: Kencana, 2024.

----------. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2018.

Jürgen Habermas, *Between Facts and Norms*, Cambridge: MIT Press, 1996

Kementerian Komunikasi dan Informatika, *Laporan Evaluasi Penanganan Insiden Siber 2023, Laporan Internal,* Jakarta, Kementerian Kominfo, 2024

Lawrence M. Friedman. *American Law: An Introduction*. New York: W.W. Norton & Company, 1984.

----------. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.

Lili Rasjidi dan I.B. Wyasa Putra. *Hukum sebagai Suatu Sistem*, Edisi Kedua. Bandung: Remaja Rosdakarya, 2020.

Lon L. Fuller, *The Morality of Law, Revised Edition*, New Haven: Yale University Press, 1969

Mahrus Ali. *Kejahatan Korporasi: Kajian Relevansi Sanksi Tindakan bagi Penanggulangan Kejahatan Korporasi*. Yogyakarta: Arti Bumi Intaran, 2018.

Marcia Baron, *Kantian Ethics Almost Without Apology*, Ithaca: Cornell University Press, 1995

Marcus K. Rogers. *Digital Forensics and Cyber Crime*, 4th Edition. New Jersey: Prentice Hall, 2020.

Martha C. Nussbaum, *Creating Capabilities*, Cambridge: Harvard University Press, 2011

Martin C. Libicki. *Cyberdeterrence and Cyberwar*. California: RAND Corporation, 2009.

Marwan Mas. *Pengantar Ilmu Hukum*. Jakarta: Ghalia Indonesia, 2018.

Maskun. *Kejahatan Siber (Cybercrime): Suatu Pengantar*. Jakarta: Kencana, 2019.

Michael J. Sandel, *Justice: What's the Right Thing to Do?,* New York: Farrar, Straus and Giroux, 2009

Mochtar Kusumaatmadja. *Konsep-konsep Hukum dalam Pembangunan*. Bandung: Alumni, 2019.

Muchsan. *Sistem Pengawasan terhadap Perbuatan Aparat Pemerintah dan Peradilan Tata Usaha Negara di Indonesia*, Cetakan Kedua. Yogyakarta: Liberty, 2020.

Muladi. *Hak Asasi Manusia: Politik dan Sistem Peradilan Pidana*. Semarang: Badan Penerbit UNDIP, 2019.

Munir Fuady. *Teori-teori Besar (Grand Theory) dalam Hukum*. Jakarta: Kencana, 2020.

Neil MacCormick, *Legal Reasoning and Legal Theory*, Oxford: Clarendon Press, 1978

Onora O'Neill, *Justice Across Boundaries*, Cambridge: Cambridge University Press, 2000

Paul Guyer, *Kant on Freedom, Law, and Happiness*, Cambridge: Cambridge University Press, 2000

Paulus Effendie Lotulung. *Beberapa Sistem tentang Kontrol Segi Hukum terhadap Pemerintah*. Jakarta: Bhuana Ilmu Populer, 2018.

Peter Mahmud Marzuki. *Penelitian Hukum*, Edisi Revisi. Jakarta: Kencana, 2019.

----------. *Pengantar Ilmu Hukum*, Edisi Revisi. Jakarta: Kencana, 2019.

Peter Singer, *Practical Ethics, 3rd Edition*, Cambridge: Cambridge University Press, 2011

Philippe Van Parijs, *Real Freedom for All*, Oxford: Oxford University Press, 1995

Philipus M. Hadjon. *Pengantar Hukum Administrasi Indonesia*, Cetakan Kesembilan. Yogyakarta: Gadjah Mada University Press, 2018.

Prajudi Atmosudirdjo. *Hukum Administrasi Negara*, Cetakan Keenam. Jakarta: Ghalia Indonesia, 2019.

Richard A. Clarke and Robert K. Knake. *Cyber War: The Next Threat to National Security*. New York: Ecco Books, 2010.

Richardus Eko Indrajit. *Cyber Intelligence dan Ketahanan Nasional*. Jakarta: Andi Publisher, 2020.

Ridwan H.R. *Hukum Administrasi Negara*, Edisi Revisi. Jakarta: Rajawali Pers, 2014.

Robert Alexy. *A Defence of Radbruch's Formula*. Oxford: Hart Publishing, 1999.

----------. *A Theory of Constitutional Rights*. Oxford: Oxford University Press, 2002.

Robert Nozick*, Anarchy, State, and Utopia*, New York: Basic Books, 1974

Robert W. Taylor. *Digital Crime and Digital Terrorism*, 5th Edition. Boston: Pearson, 2021.

Romli Atmasasmita. *Sistem Peradilan Pidana Kontemporer*. Jakarta: Kencana, 2020.

Ronald Dworkin, *Law's Empire*, Cambridge: Harvard University Press, 1986.

----------, *Taking Rights Seriously*, Cambridge: Harvard University Press, 1977

Samuel Scheffler, *The Rejection of Consequentialism, Revised Edition*, Oxford: Oxford University Press, 1994

Satjipto Rahardjo. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2000.Satjipto Rahardjo. *Ilmu Hukum*, Edisi Revisi, Cetakan VIII. Bandung: Citra Aditya Bakti, 2019.

SF Marbun. *Peradilan Administrasi Negara dan Upaya Administratif dalam Ombudsman*. Yogyakarta: FH UII Press, 2018.

Shelly Kagan, *The Limits of Morality*, Oxford: Oxford University Press, 1989

Shinta Dewi. *Cyber Law: Perlindungan Data dalam E-Commerce*. Bandung: Widya Padjadjaran, 2021.

Sjachran Basah. *Eksistensi dan Tolok Ukur Badan Peradilan Administrasi di Indonesia*. Bandung: Alumni, 2020.

Soerjono Soekanto dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Cetakan Kesepuluh. Jakarta: Raja Grafindo Persada, 2018.

Sudikno Mertokusumo. *Mengenal Hukum Suatu Pengantar*, Edisi Kelima. Yogyakarta: Liberty, 2021.

Susan W. Brenner. *Cybercrime: Criminal Threats from Cyberspace*. California: Praeger Publishers, 2010.

Suteki dan Galang Taufani. *Metodologi Penelitian Hukum*, Cetakan Kedua. Depok: RajaGrafindo Persada, 2020.

Tatiek Sri Djatmiati. *Prinsip Izin Usaha Industri di Indonesia*. Surabaya: Disertasi Universitas Airlangga, 2019.

Theo Huijbers. *Filsafat Hukum dalam Lintasan Sejarah*. Yogyakarta: Kanisius, 2017.

----------., *Dignity and Practical Reason in Kant's Moral Theory*, Ithaca: Cornell University Press, 1992.

---------- *Respect, Pluralism, and Justice*, Oxford: Oxford University Press, 2000

Thomas Pogge, *World Poverty and Human Rights, 2nd Edition*, Cambridge: Polity Press, 2008

Thomas Scanlon, *What We Owe to Each Other*, Cambridge: Harvard University Press, 1998

Tom L. Beauchamp and James F. Childress, *Principles of Biomedical Ethics, 7th Edition*, New York: Oxford University Press, 2013

Tony Honoré, *Responsibility and Fault*, Oxford: Hart Publishing, 1999

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Jurnal

Ahmad Rifai. "Implementasi Kepastian Hukum dalam Operasi Intelijen". *Law Development Journal*, Vol. 10, No. 2, 2025.

Ahmad Santoso. "Cyber Intelligence dalam Perspektif Keamanan Nasional". *Law Development Journal*, Vol. 6, No. 2, 2024.

Agus Raharjo. "Kepastian Hukum dalam Era Digital". *Jurnal Daulat Hukum*, Vol. 12, No. 1, 2025.

Anna Erliyana. "Koordinasi Kewenangan dalam Penanggulangan Kejahatan Siber". *Law Development Journal*, Vol. 9, No. 2, 2025.

Abdul Latif. "Kepastian Hukum dalam Era Digital". *Jurnal Daulat Hukum*, Vol. 7, No. 1, 2024.

Bagir Manan. "Kewenangan Atribusi, Delegasi dan Mandat dalam Hukum Administrasi". *Jurnal Daulat Hukum*, Vol. 10, No. 1, 2025.

Edy Santoso. "Sistem Peringatan Dini dalam Keamanan Nasional". *Law Development Journal*, Vol. 5, No. 2, 2022.

Hikmahanto Juwana. "Koordinasi Antar Lembaga dalam Penanggulangan Kejahatan Siber". *Law Development Journal*, Vol. 4, No. 3, 2023.

Joko Widodo. "Keamanan Siber sebagai Bagian Keamanan Nasional". *Jurnal Daulat Hukum*, Vol. 8, No. 1, 2025.

M. Yusuf Samad & Pratama Dahlian Persadha. "Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Bidang Siber". *Jurnal IPTEK dan Komunikasi (IPTEKKOM)*, BPSDMP Kominfo Yogyakarta, 2022.

Marcus Lukman. "Concurrent Authority dalam Sistem Hukum Indonesia". *Jurnal Daulat Hukum*, Vol. 11, No. 1, 2025.

Teguh Prasetyo. "Analisis Yuridis Peran BIN dalam Penanggulangan Ancaman Siber". *Jurnal Daulat Hukum*, Vol. 6, No. 1, 2023.

Widodo Muktiyo. "Perkembangan Kejahatan Siber dan Tantangan Penegakan Hukumnya". *Jurnal Daulat Hukum*, Vol. 5, No. 2, 2022.