LABORATORIUM
INDONESIA
2045

Jl. Mabes Hankam No. T65
Bambu Apus, Cipayung, 13890
lab45@lab45.id
+62 811 4520 45

Prepared statement by

Christian Guntur Lebang
Koordinator Analis Laboratorium Indonesia 2045 (LAB 45)

Disampaikan pada: Rapat Dengar Pendapat Umum (RDPU) Panitia Kerja Keamanan dan Ketahanan Siber, 7 September 2026.

***

Pada kesempatan kali ini berdasarkan kerangka acuan kerja (TOR), saya akan berfokus membahas beberapa hal, yaitu tata kelola kelembagaan; protokol eskalasi; atribusi dan asas ekstrateritorialitas; dan mekanisme pengawasan dan akuntabilitas. Adapun isu strategis lain seperti ancaman hibrida dan pengaruh asing; serta kerja sama internasional akan saya bahas secara singkat saja dalam kesempatan ini, namun bisa didiskusikan lebih jauh di sesi tanya jawab.

Saya akan menggunakan kerangka N-E-P dalam membedah regulasi keamanan siber kita, yaitu *necessity*, *effectiveness*, dan *proportionality*. Apakah regulasi tersebut perlu (*necessity*)? Apakah regulasi tersebut akan betul-betul bisa efektif bekerja (*effectiveness*)? Dan terakhir, apakah ada pengaturan kontrol yang proporsional terhadap kewenangan yang diberikan oleh regulasi tersebut (*proportionality*)?

Kerangka ini saya sadur dari Independent National Security Legislation Monitor di parlemen Australia, yang bertugas memberikan penilaian terhadap regulasi level undang-undang sektor keamanan nasional di sana.[1]

Isu pertama, *necessity*. Ini adalah diskusi yang paling sering terjadi di ruang publik. Baik pemerintah maupun DPR sudah berulang kali menyampaikan adanya kekosongan regulasi keamanan siber kita, yang berakibat pada tidak efektifnya pengamanan ruang siber, terutama yang berkaitan dengan infrastruktur kritis.

Saya tidak akan menghabiskan waktu untuk membahas ini. Saya sepakat kita membutuhkan sebuah regulasi keamanan siber, namun pertanyaan lebih jauhnya adalah regulasi seperti apa? Inilah inti dari dua isu lain, *effectiveness* dan *proportionality*.

Namun, sebelum itu saya ingin membagikan sebuah perspektif yang menarik. Saya terlibat sebagai asisten peneliti dalam proses pembentukan BSSN pada tahun 2016

[1] Independent National Security Legislation Monitor (Australia), Review of Australia's Espionage, Foreign Interference, Sabotage and Theft of Trade Secrets Offences (Division 82 and Part 5.2, Criminal Code Act 1995), 23 Juli 2026, https://www.inslm.gov.au/reviews/review-australias-espionage-foreign-interference-sabotage-and-theft-trade-secrets-offences-division-82-and-part-52-criminal-code-act-1995.

hingga 2017.[2] Sejak BSSN berdiri hingga sekarang, isu regulasi di level UU serta anggaran selalu menjadi sesuatu yang menghambat kinerjanya.

Namun uniknya, di tengah keterbatasan itu, Indonesia mencapai Tier 1 pada penilaian Global Cybersecurity Index (GCI) tahun 2024 yang lalu. Indonesia mendapatkan skor penuh, yaitu 100, dan sejajar dengan negara seperti AS, Jepang, hingga Singapura.[3] Dalam dokumen seperti RPJMN dan RKP, skor GCI Indonesia juga selalu melewati target yang ditentukan. Namun, Naskah Akademik dari RUU KKS (Keamanan dan Ketahanan Siber) yang beredar tahun lalu menyebutkan bahwa tantangannya memang bukan sekadar kerangka hukum, tetapi juga implementasi operasional dan keterbatasan sumber daya manusia.

Hal ini mengantarkan saya ke isu kedua, *effectiveness*. Apakah RUU KKS nantinya bisa betul-betul memperkuat Indonesia menghadapi ancaman dan tantangan di ruang siber yang semakin besar ke depannya?

Tata kelola kelembagaan relevan untuk didiskusikan di sini. Di TOR, disebutkan bahwa Indonesia memiliki berbagai macam K/L yang mengampu tugas masing-masing dalam ruang siber kita. Saat BSSN dibentuk, ini adalah pilihan strategis untuk tidak mengonsolidasikan semua wewenang siber dalam satu institusi. Yang kita miliki saat ini adalah pendekatan yang dikenal sebagai *whole-of-government approach*, yang diadopsi oleh berbagai negara demokratis. Pemisahan wewenang yang jelas ini menjadi landasan munculnya *trust* dengan sektor privat maupun masyarakat. Jika melihat *slide*, fungsi masing-masing institusi sebenarnya sudah cukup. Namun, potensi tumpang tindih tentu selalu ada.

Pertanyaannya adalah apakah RUU KKS memang menjawab pertanyaan ini? Jika melihat namanya, saya sempat menduga RUU ini akan betul-betul membenahi tata kelola keamanan siber dan memperjelas hubungan antarlembaga. Sebagai contoh, revisi UU TNI tahun lalu memberikan tugas baru OMSP Siber, dan saya berharap hubungan fungsi tersebut dengan institusi lain akan diperjelas di RUU ini. Namun, dari draf yang beredar sepertinya RUU ini ingin berfokus terhadap perlindungan infrastruktur kritis serta kategori baru yang disadur dari EU Cyber Resilience Act (EU CRA). Memang fungsi koordinasi untuk berbagai topik sudah dibahas dan cukup jelas akan dijalankan oleh BSSN. Namun sebagai pelaksana, muncul pertanyaan seberapa efektif BSSN bisa menjalankan fungsi koordinasi tersebut?

Berkaitan dengan ini, pertanyaan lebih jauh apakah Indonesia perlu memisahkan tiga fungsi utama: siapa pelaksana teknis, siapa yang bertanggung jawab untuk kebijakan, dan siapa yang memiliki fungsi koordinasi sekaligus memberikan sinyal politik dari pimpinan tertinggi? Amerika Serikat memisahkan ketiganya ke tiga lembaga berbeda, dengan fungsi koordinasi strategis melekat di kantor kepresidenan. Contoh negara lain bisa dilihat di *slide*. Tentu, konteks kelembagaan

[2] BSSN adalah Badan Siber dan Sandi Negara, yang dibentuk oleh Presiden Joko Widodo tahun 2017.
[3] International Telecommunication Union, *Global Cybersecurity Index 2024*, 5th ed. (Geneva: ITU, 2024), https://www.itu.int/pub/D-HDB-GCI.01-2024.

Indonesia berbeda. Tetapi saya merasa ini adalah sesuatu yang layak didiskusikan sebagai bagian dari isu tata kelola.

Isu atribusi dan ekstrateritorialitas juga sangat erat kaitannya dengan efektivitas. Apakah Indonesia betul-betul bisa menarget aktor-aktor ancaman siber dengan adanya RUU KKS? Atribusi tidak hanya bersandar pada kerangka regulasi, tetapi juga pertanyaan politik dan diplomasi, terutama ketika pelakunya adalah peretas yang disokong pemerintahan negara lain.[4] Selain itu, apakah aparat kita memang memiliki kemampuan untuk melakukan proses penegakan hukum terhadap aktor yang berasal dari luar negeri, terlepas dari pengaturan pidana di RUU KKS?

Kemudian, berdasarkan draf yang saya baca, RUU ini memandatkan setidaknya 10 topik diatur lebih jauh dalam peraturan pemerintah, termasuk topik krusial seperti penyelenggaraan dan audit teknis IIK.[5] Padahal, kita juga melihat preseden lambatnya pemerintah membahas peraturan turunan untuk UU PDP. Saat ini, hampir dua tahun dari *deadline* transisi UU tersebut, PP turunannya belum dirilis ke publik.[6] Jika hal ini terulang kembali, apakah nantinya RUU KKS akan betul-betul bisa efektif di tengah kegentingan dan perkembangan ancaman siber?

Selanjutnya, di antara efektivitas dan proporsionalitas terdapat isu protokol eskalasi. Saat ini kerangka regulasi utama di ruang siber adalah Perpres mengenai Manajemen Krisis Siber. Terdapat tiga fase generik: sebelum, saat, dan setelah krisis – yang kemudian diadopsi oleh RUU KKS. Permasalahannya, rezim eskalasi yang sudah ada ini tidak diaktifkan oleh pemerintah (dalam hal ini Presiden) saat terjadi insiden *ransomware* yang menyerang PDNS pada 2024 yang lalu. Padahal, insiden itu dalam konteks Indonesia sepertinya sudah memenuhi standar sebuah krisis siber.

Artinya, kita bisa mendiskusikan detail eskalasi insiden siber, namun perlu diciptakan mekanisme lain yang tidak hanya bergantung pada keputusan eksekutif. Belum lagi, dalam situasi krisis biasanya aktor pemerintah akan diberikan mandat wewenang lebih, yang dalam sebuah negara demokrasi seharusnya hadir bersamaan dengan akuntabilitas. RUU saat ini tidak menghadirkan mekanisme kontrol dari luar pemerintah untuk melakukan penilaian terhadap sebuah krisis siber. Tidak ada klausul pembentukan badan independen, tidak ada kewenangan kepada DPR untuk mengaktifkan mekanisme *review*.

---

[4] Lebih jauh mengenai atribusi siber bisa lihat Gatra Priyandita, "Silence as Strategy: Southeast Asia and China's Persistent Cyber Campaigns," *The Strategist* (ASPI), 1 September 2025, https://www.aspistrategist.org.au/silence-as-strategy-southeast-asia-and-chinas-persistent-cyber-campaigns/; Virpratap Vikram Singh, "Reframing Cyber Attribution," *Charting Cyberspace*, IISS, 18 Desember 2025, https://www.iiss.org/online-analysis/charting-cyberspace/2025/12/reframing-cyber-attribution/; Louise Marie Hurel dan Prerana Joshi, "Public Cyber Attribution in the Global South: Indo-Pacific," RUSI Insights Papers, 24 Maret 2026, https://www.rusi.org/explore-our-research/publications/insights-papers/public-cyber-attribution-global-south-indo-pacific.

[5] IIK adalah infrastruktur informasi kritis, sepertinya menggantikan istilah IIV (infrastruktur informasi vital).

[6] Disahkan pada Oktober 2022, UU PDP memiliki masa transisi selama dua tahun.

Untuk ini, ada pembelajaran dari AS[7] dan Australia.[8] Keduanya sudah mencoba membangun mekanisme peninjauan pasca-insiden dan pelajarannya sederhana: badan yang lahir dari keputusan eksekutif bisa dibubarkan tanpa proses legislatif, sementara badan yang dikunci undang-undang pun masih bisa disandera lewat persetujuan menteri di setiap kasus.

Bagi saya, diskusi ini relevan dengan insiden PDNS yang lalu. Hingga saat ini publik tidak mendapatkan kejelasan mengenai kegagalan yang terjadi pada insiden tersebut, padahal masyarakat luas jelas dirugikan. Ini alasan yang cukup kuat untuk menghadirkan mekanisme eksternal bagi akuntabilitas fungsi eksekutif dalam RUU KKS.

Hal ini mengantarkan kita pada isu *proportionality*.

Ada sebuah frasa yang saya dapatkan dari film "Watchmen": *quis custodiet ipsos custodes. Who watches the watchers*? Siapa yang bisa mengawasi mereka yang memiliki fungsi pengawasan? Semakin besar kewenangan yang diberikan kepada pengawas, seharusnya *oversight* yang dilakukan terhadap mereka juga semakin besar.

Misalnya, ada pembahasan kewajiban operator infrastruktur kritis untuk melakukan integrasi sistem keamanannya dengan NSOC yang dioperasikan oleh BSSN.[9] Disebutkan bahwa ketentuan ini untuk menghadapi ancaman siber dengan lebih terintegrasi. Namun, ketentuan ini tidak lazim ditemukan dalam tata kelola keamanan siber di berbagai negara demokratis. Proses berbagi informasi ancaman siber dari operator ke pemerintah berbeda dengan mengintegrasikan sistem keamanan dengan jaringan pemerintah.

Draf yang beredar memang mengisyaratkan pembahasan lebih jauh dalam Peraturan Pemerintah. Namun, klausul yang masuk dalam kategori *extraordinary* seperti ini semestinya bisa diberikan batasan-batasannya di level UU. Misal, sedalam apa integrasi tersebut? Apakah data masuk yang dianggap bukan anomali atau ancaman – yang pasti mayoritas – memiliki masa retensi oleh BSSN? Apakah

---

[7] Amerika Serikat membentuk Cyber Safety Review Board lewat Executive Order 14028 (2021), di dalam Department of Homeland Security. Anggotanya merangkap jabatan di institusi asal, termasuk perwakilan industri yang berpotensi berkonflik kepentingan dengan entitas yang diinvestigasi. Board merilis tiga laporan investigasi — Log4j (2022), Lapsus$ (2023), Storm-0558/Microsoft Exchange (2024). DHS membubarkan Board lewat memo internal, Januari 2025, di tengah investigasi Salt Typhoon yang tidak pernah dipublikasikan hasilnya. Kongres sempat mendorong kodifikasi CSRB menjadi undang-undang.

[8] Cyber Incident Review Board di Australia diatur dalam Cyber Security Act 2024 dan mulai beroperasi 2026 — keberadaannya tidak bergantung eksekutif yang sedang berkuasa. Namun pengaktifan tiap kasus tetap memerlukan persetujuan Menteri Cyber Security atas kerangka acuan investigasi. Kajian legislatif Parlemen Australia memperingatkan menteri berpotensi menunda persetujuan itu hingga investigasi kehilangan relevansi.

[9] NSOC adalah *National Security Operations Center* atau pusat pemantauan keamanan siber nasional.

ada klausul data yang didapat oleh BSSN akan bebas dari kemungkinan menjadi bahan bukti penyelidikan perkara (seperti klausul di Australia)?[10]

Begitu juga dengan topik PDED (produk dengan elemen digital). RUU akan memberikan BSSN wewenang untuk melakukan klasifikasi risiko, penilaian, pendaftaran, dan sertifikasi sekaligus. Menggunakan lensa proporsionalitas, ketentuan bahwa PDED yang sudah memenuhi standar internasional tetap perlu melakukan sertifikasi akan menjadi hambatan bagi sektor privat tanpa alasan yang jelas. Belum lagi tidak dijelaskan mekanisme sanggahan terhadap hasil penilaian tersebut.

PDED adalah terminologi baru yang kompleks dan bisa didiskusikan lebih jauh di sesi tanya jawab. Yang perlu dicatat, Uni Eropa sebagai pelopornya sendiri tengah melakukan amandemen terhadap CRA sejak akhir tahun lalu.[11] Ini topik yang masih bergerak, sehingga perlu pemahaman holistik sebelum diadopsi ke regulasi kita.

Dua catatan terakhir dari saya. Pertama, saya merasa RUU KKS bukanlah tempat yang tepat untuk membahas isu operasi informasi, CIB[12], dan operasi pengaruh asing. Ketiganya memerlukan kerangka regulasi khusus, apalagi saat ini tengah bergulir pembahasan RUU Spionase dan Intervensi Asing. Adapun ancaman hibrida yang dipahami secara luas memang memasukkan isu keamanan siber dan ketahanan infrastruktur kritis. Namun dalam kerangka regulasi kita, ancaman hibrida diatur berdasarkan UU PSDN dan Jakumhanneg[13] yang dihadapi dengan

---

[10] Australia mengatur *limited use obligation* dalam Cyber Security Act 2024, yang membatasi penggunaan informasi insiden yang diterima pemerintah agar tidak dipakai untuk penegakan hukum terhadap pihak pelapor. Lihat Department of Home Affairs, Australia, *Factsheet: Limited Use for the National Cyber Security Coordinator*, Part 4 Cyber Security Act 2024. https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-limited-use-ncsc.pdf.

[11] Komisi Eropa mempresentasikan Digital Omnibus Package pada 19 November 2025, mengusulkan portal pelaporan insiden tunggal (dikelola ENISA) untuk menyederhanakan kewajiban lapor lintas GDPR, NIS2, DORA, CER, dan Cyber Resilience Act — menaikkan ambang ke insiden berisiko tinggi dan memperpanjang tenggat menjadi 96 jam. Per pertengahan 2026, paket ini masih dalam proses legislatif biasa di Parlemen dan Dewan Eropa, belum disahkan final. European Commission, "Digital Omnibus Package," 19 November 2025, https://digital-strategy.ec.europa.eu/en/policies/digital-omnibus; lihat juga Jones Day, "EU Digital Omnibus: How EU Data, Cyber, and AI Rules Will Shift," 18 Desember 2025, https://www.jonesday.com/en/insights/2025/12/eu-digital-omnibus-how-eu-data-cyber-and-ai-rules-will-shift.

[12] Meta merumuskan istilah Coordinated Inauthentic Behaviour (CIB) pada 2019 untuk menggambarkan penggunaan banyak akun secara terkoordinasi, termasuk akun palsu, guna menyesatkan publik. Istilah ini kemudian dipakai lebih luas untuk operasi pengaruh asing, termasuk oleh European External Action Service (EEAS) dalam kerangka Foreign Information Manipulation and Interference (FIMI). EU DisinfoLab, "Disinformation Glossary: 150+ Terms to Understand the Information Disorder," https://www.disinfo.eu/publications/disinformation-glossary-150-terms-to-understand-the-information-disorder/.

[13] Undang-Undang Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara; Peraturan Presiden Nomor 111 Tahun 2025 tentang Kebijakan Umum Pertahanan Negara Tahun 2025-2029.

gelar militer dan dikoordinasikan oleh Kementerian Pertahanan. Ini akan menjadi topik yang lebih besar lagi terkait arsitektur respons Indonesia.

Kedua, terkait kerja sama internasional, saya tadi sudah menyinggung keterbatasan kapasitas atribusi kita. Bagian kerja sama internasional dalam draf yang beredar juga hanya memuat dua ayat yang sangat umum. Namun terlepas dari itu, ada pertanyaan lebih besar mengenai isu keamanan siber dan pilihan vendor infrastruktur teknologi. Keduanya semakin tidak bisa dilepaskan dari persaingan geopolitik dunia yang membutuhkan visi yang jelas dan lebih besar dari sekadar pengaturan tata kelola keamanan siber dan detail teknisnya.

Sebagai penutup, saya berterima kasih atas kesempatan untuk menyampaikan pandangan saya ini. Beberapa waktu lalu saya menulis di harian Kompas pentingnya pembahasan RUU KKS secara transparan, karena dengan begitu *trust* bisa terbangun terhadap pemerintah di sektor ini. Saya berharap ke depannya, pembahasan ini bisa terus terbuka dan draf resmi bisa segera dipelajari oleh publik.

Sekian dari saya dan terima kasih atas perhatian Ibu dan Bapak sekalian.