**Ketahanan Siber Indonesia: Indonesia di Pusat Pertumbuhan Ekonomi Digital ASEAN**

*Dr. Kartina Sury, Senior Fellow di Center for Indonesian Policy Studies (CIPS), mengkaji kesenjangan dan tantangan yang dihadapi Indonesia dalam mengatasi ancaman keamanan siber dan menyampaikan rekomendasinya. Artikel ini mengacu pada penelitian terbaru dari Tech For Good Institute (TFGI) tentang ketahanan siber.*

Riset Ketahanan Siber dari TFGI


*oleh Dr. Kartina Sury, Senior Fellow di Center for Indonesian Policy Studies*

Dengan nilai transaksi digital Indonesia yang mencapai $77 miliar (atau 40% dari total wilayah negara) pada tahun 2022, Indonesia terus menempatkan posisinya sebagai pemain utama dalam ekonomi digital di Asia Tenggara (ASEAN). Nilai total transaksi digital diproyeksikan akan berlipat ganda menjadi $130 miliar pada tahun 2025, yang lebih lanjut mengukuhkan Indonesia sebagai kontributor signifikan bagi ekonomi digital yang dinamis di wilayah ini. Selain itu, Indonesia mendorong ekosistem rintisan (*startup*) yang sehat dan menduduki peringkat ke-6 secara global dalam hal jumlah perusahaan rintisan terbanyak, dengan lebih dari 2.400 perusahaan rintisan. Dalam beberapa tahun mendatang, Indonesia terus memprioritaskan transformasi digital sebagai salah satu prioritas nasional.

Namun, percepatan digitalisasi di Indonesia juga meningkatkan risiko terhadap tantangan seperti ancaman siber. Ini mencakup risiko pelanggaran data di lembaga pemerintah, badan usaha milik negara, dan sektor jasa keuangan yang berpotensi membawa dampak bagi jutaan pelanggan/nasabah. Sebagai contoh, kebocoran data dan pencurian identitas adalah kekhawatiran utama yang berkontribusi sekitar 88% dari serangan siber yang terjadi dalam tiga tahun terakhir. Laporan Kementerian Komunikasi dan Informatika (Kominfo) di tahun 2021 mengungkapkan bahwa 93% dari kasus kebocoran data disebabkan oleh permasalahan keamanan siber. Hal ini menggarisbawahi perlunya Indonesia untuk melakukan berbagai upaya yang akan mendorong peningkatan ketahanan siber.

**Tantangan Bagi Ketahanan Siber Indonesia**

Ketahanan siber Indonesia menjadi perhatian akibat ketidakpastian dalam kesiapannya akan transformasi digital di berbagai industri. Pada tahun 2022, Badan Siber dan Sandi Negara (BSSN) mencatat hampir satu miliar serangan siber, dengan lebih dari separuh serangan terkait *malware*, serangan kebocoran data berkontribusi sebesar 15%, dan aktivitas *trojan* tercatat sekitar 10%. Lebih lanjut, di pertengahan pertama tahun 2023 saja, Indonesia tercatat telah mengalami lebih dari 347 juta kasus serangan siber, dengan jumlah kasus tertinggi disebabkan oleh insiden *ransomware.*

Selain ancaman serangan siber, tentunya terdapat ruang untuk memperbaiki dan menyempurnakan kerangka regulasi di Indonesia. Saat ini, hukum yang terkait dengan ketahanan siber masih bersifat terpisah. Sebagai contoh:

- Peraturan Pemerintah No. 71/2019 fokus pada kejahatan siber terkait transaksi elektronik, namun mengabaikan serangan terhadap infrastruktur yang kritis
- Peraturan Kementerian Pertahanan (Kemenhan) No. 82/2014 membahas pertahanan siber militer tetapi tidak mencakup keamanan siber publik
- Rencana Strategis 2020–2024 Kementerian Komunikasi dan Informatika membagi tanggung jawab antara Kominfo dan BSSN untuk pertahanan siber dan perlindungan data pribadi. Rencana ini mencakup kerangka kerja untuk teknologi yang tengah berkembang seperti kecerdasan buatan (*Artificial Intelligence*) dan pembelajaran mesin (*machine learning*), serta pentingnya layanan pemerintah berbasis elektronik dan implementasi teknologi seperti *big data*, pembelajaran mesin, dan *blockchain*. Namun, langkah-langkah tindakan spesifik untuk mendukung *e-government* (penyelenggaraan pemerintahan berbasis elektronik) tidak dijelaskan dengan terperinci, kecuali hal terkait kebutuhan untuk berkolaborasi di berbagai tingkat pemerintahan.
- Keputusan Presiden No. 47/2023 menekankan pada Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, dan bagian dari tujuan utama adalah melindungi ekosistem ekonomi digital nasional, meningkatkan kekuatan dan kemampuan ketahanan Keamanan Siber, serta memprioritaskan kepentingan nasional sejalan dengan upaya untuk mendukung terciptanya ranah siber global. Namun demikian, masih ada kebutuhan tata kelola lebih lanjut dalam menerapkan Risiko dan Mitigasi Siber.

Pemangku kepentingan yang terlibat dalam Manajemen Krisis Siber, khususnya Penyedia Sistem Elektronik (PSE), membutuhkan instruksi pelaksanaan yang lebih komprehensif dan perencanaan teraudit untuk melindungi para konsumen.

Kajian CIPS mengungkapkan beberapa kekurangan, termasuk kebutuhan akan sumber daya manusia berkompeten diranah Kominfo, mekanisme tanggapan yang terstandarisasi, regulasi bersama perwakilan non-pemerintah, serta memperjelas mandat antara lembaga-lembaga kementerian.

Dalam hal perlindungan data pribadi, regulasi ini masih belum memaparkan dengan jelas dalam hal bagaimana masyarakat menerima informasi dalam kasus kejahatan siber atau pelanggaran data. Mekanisme komunikasi masih kurang jelas selain ketentuan dari Otoritas Jasa Keuangan (OJK) yang mengatur pelaporan keuangan tahunan dan triwulanan. Selanjutnya, tidak ada pemahaman yang konsisten mengenai langkah-langkah praktis bagi bisnis, konsumen/nasabah, dan organisasi untuk menerapkan dan meningkatkan keamanan siber.

**Menuju Perbaikan Ketahanan Siber di Indonesia**

Terdapat beberapa pertimbangan utama bagi Indonesia untuk memperkuat posisi keamanan sibernya. Rekomendasi kebijakan ini bertujuan untuk meningkatkan kemampuan negara untuk beradaptasi terhadap ancaman siber yang terus berkembang.

| **1. Penyelarasan kebijakan keamanan siber di ruang lingkup domestik dan internasional.** |
| --- |
| ● Membentuk Badan Siber Nasional untuk meningkatkan ketahanan siber sejalan dengan pertumbuhan ekonomi digital.<br>● Mengklarifikasi kebijakan data dan jaringan untuk perlindungan dan keamanan data pribadi melalui panduan cetak biru standar, memfasilitasi tanggapan efektif dari berbagai lembaga pemerintah.<br>● Membentuk kerangka dan tata kelola untuk insiden pelaporan, pengelolaan, dan kajian paska insiden siber, yang harus dipatuhi oleh para pemangku kepentingan. Hal ini mencakup tata kelola data pribadi dan mitigasi untuk tercapainya ranah siber yang terbuka, aman, stabil, dan bertanggung jawab.<br>● Menjalin kemitraan internasional untuk menanggulangi sifat serangan siber yang selalu berubah. Terkait hal ini, penting untuk memanfaatkan Strategi Kerja Sama Keamanan Siber ASEAN 2021-2025 untuk mengadopsi langkah-langkah siber yang standar dan terukur, termasuk berbagi informasi, koordinasi, implementasi norma, program membangun kapasitas, dan keterlibatan multilateral.<br>● Peraturan Pemerintah No. 27/2022 telah diberlakukan dan secara resmi dilaksanakan; akan tetapi, dua tahun masa transisi diterapkan untuk pengendali data pribadi. Oleh |

karena itu, sangat penting untuk memastikan penerapan lengkap Data Pribadi, dan kerangka kebijakan data harus diperkenalkan untuk melindungi negara.
- Mempertimbangkan untuk memasukkan pendekatan kerangka ketahanan TFGI ke dalam pengembangan kerangka untuk Indonesia, memperkuat ketahanan siber dalam aspek perlindungan, identifikasi, deteksi, tanggapan, dan adaptasi.

**2. Pendekatan menyeluruh ke masyarakat sangat penting bagi ketahanan siber Indonesia.**

- Menciptakan platform bagi sektor swasta dan organisasi masyarakat sipil untuk berbagi wawasan dan pandangan tentang keamanan siber. Kolaborasi di antara para pemangku kepentingan utama dapat membantu melindungi infrastruktur kritis dari serangan siber, meningkatkan privasi data pribadi, dan melindungi konsumen/nasabah.
- Regulasi keamanan siber sektoral terkait e-commerce, sektor keuangan, dan industri lainnya yang relevan, yang dalam kegiatannya melibatkan pengumpulan data dalam aktivitas bisnis sehari-hari harus mengimplementasikan mekanisme yang jelas untuk koordinasi, pelaporan, dan penyelesaian insiden siber.
- FBagi bisnis, mendorong investasi dalam teknologi keamanan siber dapat menarik pendanaan dan membangun kepercayaan dan keyakinan konsumen/nasabah.
- Bagi pemerintah, penting untuk mempertimbangkan kerangka rinci tentang pendekatan berbasis risiko terhadap klasifikasi data, sebagai pedoman yang harus dipatuhi oleh pemangku kepentingan.
- Seperti yang telah digaris bawahi oleh Asosiasi Jasa Keuangan dan Pembayaran di Indonesia, kerjasama antara regulator dan pelaku industri dapat membantu membangun ketahanan siber Indonesia.

**3. Meningkatkan tenaga kerja keamanan siber melalui literasi digital dan edukasi siber.**

- Mengintegrasikan upaya literasi digital di berbagai kementerian seperti Kominfo serta Kementerian Pendidikan dan Kebudayaan sangatlah penting. Hal ini melibatkan perbaikan pendidikan dari jenjang pendidikan dasar 12 tahun hingga universitas. Peningkatan keterampilan para guru melalui pelatihan komprehensif juga penting. Bisnis dan asosiasi industri dapat menyediakan materi teknis kepada masyarakat untuk pemahaman yang lebih baik akan teknologi digital.
- Literasi digital memperkuat ketahanan siber. Kesadaran masyarakat dan keterampilan keamanan siber menjadi penting. Bisnis, regulator, dan masyarakat harus mengintensitaskan kampanye informasi publik tentang perlindungan data.
- Meskipun potensi ekonomi digital sangat mengesankan, Indonesia masih kekurangan sumber daya digital sebagai pintu utama untuk membuka jalan bagi tumbuhnya

sumber daya di bidang keamanan siber. Hal ini memerlukan kerjasama yang efektif dari program-progam lintas kementerian.

- Menyampaikan permasalahan kekurangan para profesional yang kompeten di sektor keamanan siber menjadi hal yang mendesak. Meningkatkan jalur pendidikan, imigrasi, dan akreditasi dapat sejalan dengan terbentuknya Badan Siber Nasional.

Dengan demikian maka dapat disimpulkan bahwa membangun ketahanan siber adalah faktor penting bagi Indonesia untuk mempertahankan posisinya sebagai pusat utama ekonomi digital di Asia Tenggara. Untuk meningkatkan ketahanan, menyelaraskan regulasi siber, membangun Badan Siber Nasional, dan menerapkan cetak biru yang standar untuk perlindungan data sangatlah penting. Kemitraan internasional akan memperkuat kemampuan Indonesia untuk menanggulangi ancaman dan kerentanan siber. Sangat penting untuk mendorong pendekatan menyeluruh terhadap masyarakat melalui penciptaan landasan di mana pemerintah, bisnis dan masyarakat sipil dapat bekerjasama. Sebagai penutup, mempromosikan literasi digital dapat membantu menanggulangi kekurangan akan profesional keamanan siber dan juga meningkatkan kewaspadaan masyarakat akan risiko yang berhubungan dengan siber.

**Tentang penulis**

*Dr. Kartina Sury, Senior Fellow di Center for Indonesian Policy Studies. Minat risetnya adalah di ruang lingkup Ekonomi Digital, Pendidikan Keuangan, Literasi Digital dan Literasi Keuangan Digital serta Inklusi, Perlindungan Konsumen.*