Komisi I

BUDGET ISSUE BRIEF

Vol. 02, Edisi 16, September 2022 Edisi Magang Di Rumah Rakyat Tahun 2022

Tantangan Penanganan Ancaman Siber dalam Menyongsong Pemilihan Umum 2024

HIGHLIGHT

- Perkembangan teknologi yang di Indonesia dalam rangka memasuki era transformasi digital harus ditingkatkan untuk menjaga keamanan dari ancaman siber.
- anomali trafik yang terjadi di Indonesia, mengalami jumlah peningkatan yang signifikan dari tahun ke tahun (2019-2022). Jika tidak ada penanganan siber maka akan menganggu pemilu di 2024
- Anggaran dari BSSN, yang merupakan lembaga secara khusus untuk menangani keamanan siber sebesar Rp624,4 miliar dinilai masih belum cukup untuk membiayai program strategis BSSN.
- Kebutuhan anggaran yang tidak terpenuhi dapat mengakibatkan adanya ancaman siber yang dapat berdampak pada keamanan pemilu, yang harus diperhatikan oleh pemerintah antara lain; 1) Pemerintah harus segera mengesahkan UU yang spesifik dan lengkap mengenai kejahatan siber 2) penguatan anggaran 3) Mempersiapkan Sumber Daya Manusia dengan edukasi dan pelatihan 4) Belajar dari pemilu 2019 dengan lebih mengefektifkan *collaborativeapproach*

PUSAT KAJIAN ANGGARAN
Badan Keahlian, Sekretariat Jenderal DPR RI

Pengarah
Dr. Inosentius Samsul, S.H., M.Hum.
Penanggung Jawab
Drs. Helmizar, M.E.

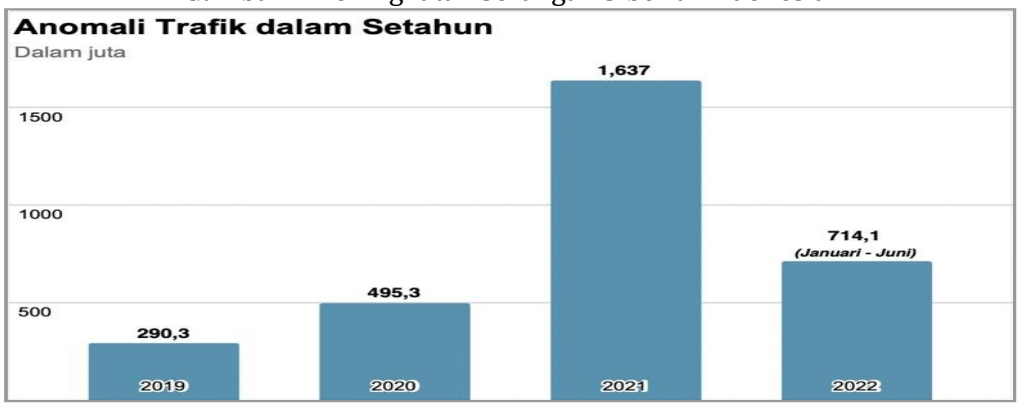
Redaktur:
Rendy Alvaro · Ade Nurul Aida

Penulis: Ardimansyah, Arya Sebastian, Carlence Maurlen, Elsya, Nova Afidatunnisa

Salah satu dampak buruk yang timbul pada perkembangan teknologi dalam era globalisasi adalah penyalahgunaan teknologi oleh oknum yang tidak bertanggung jawab yang melibatkan jaringan komputer. Penguatan keamanan siber sangat penting untuk mengurangi dan mengatasi risiko siber, dimana besarnya urgensi keamanan siber berkaitan langsung dengan tingkat ketergantungan penggunaan di ruang siber.

Seiring dengan pertumbuhan teknologi, ancaman siber terus mengalami peningkatan yang sangat pesat. Berdasarkan laporan monitoring BSSN, tingkat serangan siber di tahun 2019 mencapai 290,3 juta. Angka tersebut terus mengalami peningkatan hingga di tahun 2021 yang mencapai 1,637 juta. Kemudian hingga Juni 2022 serangan siber juga telah mencapai 714,1 juta.

Gambar 1. Peningkatan Serangan Siber di Indonesia



Sumber: Laporan Monitoring BSSN (diolah)

Sementara itu, perusahaan keamanan siber Kaspersky mencatat terdapat 11 juta serangan siber yang terjadi di Indonesia pada kuartal pertama tahun 2022. Puncak serangan siber pada tahun ini disebabkan adanya kebocoran 1,3 miliar data nomor telepon dan NIK milik masyarakat Indonesia. Kemudian terdapat kebocoran data PLN seperti ID pelanggan, nama dan alamat konsumen, informasi terkait besarnya penggunaan listrik dalam kWH, hingga tipe energi yang digunakan. Kasus lain adanya kebocoran data IndiHome yang mengandung riwayat pencarian internet pelanggan. Selain itu, terdapat pula kasus siber dimana NIK masyarakat Indonesia terdaftar sebagai anggota partai politik di Sistem Informasi Partai Politik (SIPOL) tanpa diketahui sebelumnya. Dampak dari hal tersebut adalah mereka tidak bisa menjadi penyelenggara pemilu. Apabila kasus ini tidak kunjung teratasi, akan menghambat jalannya pemilu yang akan datang.

Ancaman siber pada penyelenggaraan pemilu sebelumnya pernah terjadi. Ancaman terhadap keamanan siber/ kejahatan siber pada tahun 2019 yang disidik oleh Kepolisian RI mencapai 2.800 kasus, dimana lebih dari 35% (1.005 kasus) terjadi pada saat kampanye pemilihan umum (Kompas.com). Lonjakan kasus tersebut dimulai pada bulan September 2018 saat proses kampanye dimulai. Bentuk kasus *cyber crime* yang terjadi berupa ujaran kebencian, penyebaran hoaks, dan pengancaman. Pemilihan umum sendiri merupakan hal yang vital dan kritis sebagai pilar demokrasi dalam penyelenggaraan pemerintahan suatu negara. Akibatnya, setiap gangguan dalam penyelenggaraan pemilu dapat menimbulkan gejolak politik, ketidakstabilan keamanan dalam negeri, dan ancaman terhadap pertahanan negara.

Keamanan siber harus tetap diterapkan selama pengembangan sistem teknologi manajemen pemilu, khususnya untuk penyelenggaraan pemilu kedepannya terlebih ketika memasuki era transformasi digital, dimana ruang siber harus memiliki kekuatan agar tercipta suasana yang tertib dan kondusif. Oleh karena itu, Indonesia harus memiliki komponen pendukung dalam rangka peningkatan keamanan dan perlindungan dari ancaman siber serta bentuk pengaksesan ilegal.

Tantangan Penanganan Ancaman Siber

Regulasi. Menuju tahun 2024 Indonesia akan mengadakan pemilihan umum serentak untukmemilih pemimpin yang baru dengan harapan tingkat keamanan siber harus segera diimplementasikan. Indonesia dinilai masih belum memiliki regulasi yang jelas terkait payung hukum atau undang-undang yang mengatur tentang kejahatan siber. Menanggapi situasi genting yang akan dihadapi oleh Indonesia di pemilihan umum kedepannya, dapat dilihat dari Undang-Undang yang dapat menangani kasus kejahatan siber. Dilansir dari akademis Sunkho et al., (2018), faktanya hanya Indonesia dari keenam negara ASEAN (Indonesia, Malaysia, Filipina, Singapura, Thailand, dan Vietnam) yang tidak memiliki UU dalam menangani keamanan dan ketahanan siber secara khusus.

Tabel 1. UU Tentang Keamanan Siber Negara ASEAN

Negara	*Cybercrime Prevention*	Bentuk Pelanggaran
Indonesia	*No Specific Cybersecurity Laws*; UU ITE No. 11 Tahun 2008	Judicial System
Malaysia	Computer Crime Act 1997	Notice and takedown
Philippines	Cybercrime Prevention Act (2012)	Judicial System
Singapore	COMPUTER MISUSE ACT (1993, amended 2017)	Notice and takedown
Thailand	Computer-Related Crime Bill (2007, amended 2017)	Judicial System
Vietnam	Law on Cyber Informasi Security (Law No. 86/2015/QH13)	Judicial System

Sumber: Sunkho et al, (2018)

Anggaran. Untuk menjaga stabilitas keamanan maka dibutuhkan suatu modifikasi agar pengelolaan jaringan akan berjalan dengan baik. Pada RAPBN tahun 2023, anggaran diberikan untuk BSSN yang merupakan lembaga khusus untuk menangani keamanan siber sebesar Rp624 miliar, sedangkan Kepala BSSN menyebutkan bahwa anggaran dibawah Rp1 triliun tergolong kurang untuk merealisasikan pertahanan siber. Anggaran yang telah diberikan masih dinilai sangat kurang untuk menciptakan keamanan siber yang optimal di Indonesia. Selain itu, berdasarkan data A.T Kearney (2018) menunjukkan, bahwa pada tahun 2017 anggaran belanja keamanan siber Indonesia hanya mencapai USD1.829 juta atau setara degan 0,02 persen dari GDP. Besaran angka tersebut masih jauh diantara beberapa negara asean seperti Singapura, Malaysia, Thailand, Vietnam, Filipina, bahkan rata-rata negara ASEAN maupun rata-rata global.

Sumber Daya Manusia (SDM). SDM yang kompeten dalam bidang siber masih sangat minim. Ketua Indonesia Cyber Security Forum (ICSF) menyatakan bahwa saat ini keamanan siber nasional memerlukan sekitar 10.000 SDM setiap tahunnya. Kebutuhan ini berada pada tingkatan engineer dan analyst. Jumlah ini tidak berbeda jauh dengan jumlah kebutuhan yang diperkirakan oleh Menteri Komunikasi dan Informatika. Dimana dalam kurun waktu 15 tahun, Indonesia memerlukan 9 juta talenta digital. Jumlah ini akan terus mengalami pertumbuhan rata-rata 600.000 talenta digital setiap tahunnya pada semua level keahlian. Tingginya kebutuhan talenta digital, saat ini belum diikuti dengan ketersediaan sumberdaya manusia.

Penutup

Penerapan pertahanan siber menjadi keniscayaan dan merupakan suatu prioritas kewajiban bagi negara dan semua instansi di dalamnya dimana tingkat pentingnya berbanding lurus dengan tingkat ketergantungan pada pemanfaatan di ruang siber tersebut. Terutama dalam persiapan Indonesia tahun 2024 mendatang. Oleh karena itu terdapat beberapa poin yang perlu dipertimbangkan antara lain: **Pertama,** Pemerintah harus segera mengesahkan payung hukum atau UU yang spesifik dan lengkap mengenai ancaman siber, dari data terdapat perbedaan aturan yang diterapkan di negara ASEAN. Dapat kita lihat bahwa dari keenam negara hanya Indonesia yang tidak memiliki undang-undang keamanan siber secara khusus karena aturan di Indonesia hanya mengandalkan UU ITE dan pemerintah yang masih memproses dan mengkaji RUU tentang Perlindungan Data Pribadi (PDP). **Kedua,** perlunya penguatan anggaran, mengingat kebutuhan dari BSSN terkait keamanan siber menjelang pemilu 2024 antara lain: Rp10 miliar untuk mengamankan 10 aplikasi terkait pemilu, Rp699 miliar sebagai rekam cadang elektronik , penguatan balai sertifikat elektronik sebesar Rp49 miliar, Rp200 miliar untuk penambahan slot di provider, Rp155 miliar untuk pengembangan politeknik siber, serta Rp1 miliar untuk kebutuhan literasi serta perundang - undangan dan kesadaran hukum ketahanan siber. Sementara menurut nota keuangan 2023 untuk RAPBN 2023, pemerintah hanya memberikan anggaran sebesar Rp624,4miliar, dan angka ini dinilai tidak mencukupi, terutama dalam menghadapi pemilu tahun 2024 mendatang. Selain itu, BSSN perlu meningkatkan sinergitas dengan cara bekerja sama dengan mitra lain. **Ketiga,** mempersiapkan Sumber Daya Manusia dengan edukasi dan pelatihan**. Keempat, b**elajar dari pemilu 2019 dengan lebih mengefektifkan *collaborative approach* dengan konsep kerjasama *Triple Helix* yang melibatkan Pemerintah, Swasta dan Akademisi. Strategi tersebut meliputi deteksi, proteksi dan prevensi dari ancaman pada titik-titik kritis dan rawan pada saat sebelum, pelaksanaan dan pasca pemilu yang diharapkan dapat mendukung keberhasilan pelaksanaan pemilu mendatang.