



Accountability Brief

Pengarah:
Inosentius Samsul
(Kepala Badan Keahlian DPR RI)
Tim Penulis:
Djustiawan Widjaya
Fachry Ali Firdaus
Dwimo Gogy Prabowo

Urgensi penanganan kejahatan siber secara holistik di Indonesia

1. Latar Belakang

Berbagai aktivitas dan kegiatan yang dijalankan saat ini, mulai dari individu, perusahaan, hingga pemerintah, tidak dapat terlepas dari peranan internet. Teknologi yang ditemukan pada tahun 1983 tersebut seiring berjalannya waktu semakin terintegrasi dalam teknologi dan dalam kehidupan manusia. Saat ini tercatat lebih dari 4.9 milyar penduduk dunia yang terkoneksi ke internet, atau 62% dari total penduduk dunia. Di Indonesia pada tahun 2021 tercatat jumlah pengguna internet mencapai 202.6 juta orang, atau mencapai 73.7% (Nurhayati-Wolff, 2021). Pandemi Covid-19 yang membatasi mobilitas penduduk, mendorong berbagai aktivitas dilakukan secara daring menjadi salah satu pemacu akselerasi peningkatan pengguna internet. Kenaikan jumlah pengguna dari tahun 2019 ke tahun 2021 tercatat sangat signifikan, mencapai 52.6 juta pengguna (Annur, 2022).

Semakin meningkatnya jumlah pengguna internet pastinya akan sejalan dengan tingkat utilisasi internet. Di setiap harinya, orang Indonesia secara rerata menghabiskan hampir 9 jam waktunya menggunakan Internet. Dari waktu tersebut, lebih dari 3 jam diantaranya dihabiskan untuk bersosial media. Sosial media merupakan salah satu bagian dari fungsi internet, yaitu sebagai sarana konektivitas dan komunikasi. Selain itu internet juga berfungsi sebagai sarana untuk mengakses informasi, pengetahuan, dan edukasi; sarana alamat dan pemetaan; sarana berbisnis; dan sarana hiburan (Rhani, 2020).

Pandemi Covid-19 yang mengharuskan masyarakat sebisa mungkin melakukan aktivitasnya dengan meminimalkan kontak fisik telah mengubah gaya hidup masyarakat di berbagai negara dan peran internet juga semakin esensial. Di Amerika Serikat, berdasarkan survei yang dilakukan pewresearch, 90% orang dewasa mengatakan bahwa internet sangat penting dan esensial dalam kehidupan mereka, dan 40% diantaranya menggunakan layanan teknologi baru yang belum digunakan sebelumnya (Colleen McClain, 2021). Hal yang sama juga terjadi di Indonesia, tercermin dari kenaikan trafik internet dan trafik aplikasi. Di saat penerapan PPKM level 4, salah satu operator telekomunikasi mencatatkan kenaikan 5% dan

2022

Komisi III

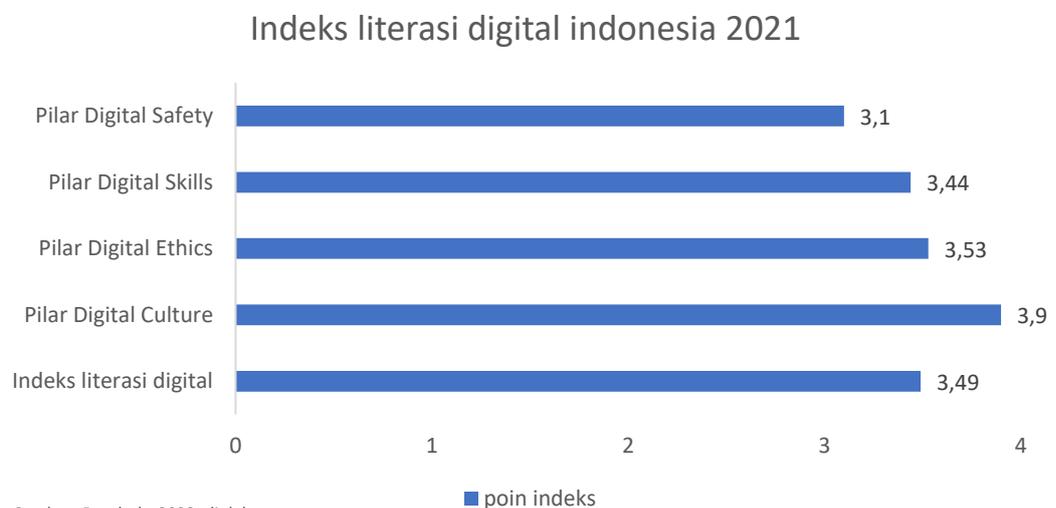
perubahan pola pemakaian dari perkantoran ke area residensial dan area pendukung penanganan pandemic covid-19 seperti Rumah Sakit (Nursyamsi, 2021).

Perubahan aktivitas ekonomi juga tercermin dari kenaikan nilai transaksi ecommerce di Indonesia yang tumbuh signifikan sebesar 63.4% mencapai Rp186.7 triliun pada semester awal 2021 (Hidayat, 2021). Transaksi digital perbankan, pengguna layanan Pendidikan daring, dan layanan teleconference juga semuanya mencatatkan kenaikan trafik signifikan selama pandemic.

Meskipun pandemi mulai mereda, beberapa perubahan yang tercipta selama pandemic besar kemungkinan akan tetap bertahan, seperti penggunaan layanan videoconference untuk rapat dan webinar, layanan telehealth, belanja daring, dan layanan Pendidikan daring, sehingga berbagai layanan yang berbasis internet tersebut akan semakin esensial dalam kehidupan masyarakat (Kantrowitz, 2021). Oleh karena itu, menjadi sebuah keniscayaan bahwa Pemerintah perlu menjamin keamanan berbagai kegiatan yang dilakukan secara daring.

2. Permasalahan

Seiring dengan semakin masifnya aktivitas sehari – hari yang dilakukan secara daring, disamping memberikan kemudahan namun juga disertai dengan peningkatan paparan risiko keamanan digital. Berdasarkan data dari BSSSN, hingga bulan Juli 2022 saja Indonesia menerima 717,170,967 anomali trafik atau serangan siber (CNN Indonesia, 2022). Kenaikan paparan risiko tersebut sayangnya belum diiringi dengan kesiapan SDM dan institusi. Berdasarkan indeks literasi digital tahun 2021, aspek keamanan digital mendapatkan skor paling rendah. Selain itu, kenaikan penetrasi internet selama pandemic juga tidak dibarengi dengan kenaikan skor indeks literasi digital yang naik sangat tipis dari 3.46 di 2020 menjadi 3.49 di 2021 (Harsono, 2022). Nilai tersebut menempatkan literasi digital masyarakat Indonesia di level menengah, belum mencapai baik. Apabila dirinci, Pilar digital safety mendapatkan skor 3.1, dan pilar dengan skor tertinggi adalah pilar digital culture dengan skor 3.9, masih dalam kategori sedang.



Secara infrastruktur institusional, kualitas keamanan digital Indonesia berdasarkan National Cyber Security Index (NCSI) berada diperingkat ke 83 di dunia. Aspek eID & TS (E-identification & Trust Services) mendapatkan nilai tertinggi dengan pemenuhan standar mencapai 89%, sedangkan aspek kebijakan dan perlindungan layanan esensial mendapatkan skor terendah yaitu 0%. Masih belum memadainya kesadaran keamanan digital masyarakat, disertai dengan infrastruktur keamanan yang belum sempurna mendorong terjadinya banyak kejahatan digital/siber.

Saat ini di Indonesia belum ada definisi hukum mengenai kejahatan siber. Dasar hukum yang digunakan mengacu pada Undang – Undang Nomor 11 Tahun 2008 yang diperbarui dengan Undang – Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) (Prahassacitta, 2019). Berdasarkan jenisnya, kejahatan siber terbagi menjadi dua kategori yaitu kejahatan yang menasar internet, perangkat, dan teknologi terkait, dan yang kedua adalah konten ilegal yang memanfaatkan internet dan teknologi terkait untuk menyelenggarakan tindak kejahatan. Tindak peretasan, pencurian data elektronik, pencurian identitas, dan fasilitasi tindak pidana terlarang termasuk kedalam kejahatan jenis pertama.

Berdasarkan laporan yang dirilis interpol, ASEAN Cyberthreat Assesment 2021, terdapat 7 jenis kejahatan siber yang menjadi tren di tahun 2020. Pada bentuk kejahatan phishing, perbankan di ASEAN menjadi target utama jenis kejahatan ini. Terdapat 749,915 serangan jenis ini yang menyerang Indonesia di 2020, menjadikan Indonesia negara dengan serangan phishing terbanyak. Pada jenis kejahatan ransomware, Indonesia juga menjadi negara yang mengalami serangan terbanyak, mencapai 1.3 juta serangan ransomware yang terdeteksi. Sektor yang diserang adalah sektor terkait sawit dan turunannya (Interpol, 2021). Kejahatan ini termasuk ke dalam jenis kejahatan kategori 1. Berdasarkan data dari laman Direktorat Tindak Pidana Siber Bareskrim Polri, di tahun 2022 saja di Indonesia terdapat 5896 laporan tindak kejahatan siber yang diterima, didominasi oleh pengancaman, dan perjudian, tindak kejahatan yang termasuk kedalam kejahatan kategori 2. Judi Online di Indonesia berdasarkan data dari PPATK di tahun 2022 saja sudah mencapai Rp155.46 triliun. PPATK dilaporkan telah berhasil membekukan 312 rekening dengan nilai mencapai Rp836 miliar. Berdasarkan data laman kredibel, sebuah laman yang membantu mengidentifikasi potensi terjadinya penipuan pada suatu transaksi daring, tercatat ada lebih dari 220 ribu laporan diterima dengan 127 ribu rekening bank yang terdeteksi penipu, dan dengan nilai kerugian mencapai Rp331,4 miliar sejak tahun 2018.

Penanganan kejahatan siber di Indonesia nampaknya masih difokuskan pada penguatan ketahanan siber dari aspek ketahanan/keamanan. Pada RKP 2022, tercatat ada 5 proyek prioritas (Pro-P) pada 2 Kegiatan Prioritas (KP) dengan dukungan anggaran mencapai Rp210.9 miliar. Selain kelima proyek prioritas tersebut juga terdapat Proyek Prioritas Pengelolaan Informasi secara Aman dan Terintegrasi di Kominfo dengan output pemblokiran konten negatif. Tercatat ada 5 Kementerian/Lembaga yang terlibat menjadi stakeholder dalam penanganan terkait ketahanan siber, yaitu Kementerian Pertahanan, BIN, BSSN, Polri, Kejaksaan, dan Kominfo. Berdasarkan buku Kebijakan Cybersecurity dalam Perspektif

Multistakeholder yang dirilis Kementerian Komunikasi dan Informatika di tahun 2018, pendekatan kebijakan penanganan siber di Indonesia berdasarkan pada fokus ancaman nasional dan perlindungan infrastruktur nasional kritis. Hal ini juga tergambar dari kementerian/lembaga yang terlibat yaitu Kominfo, Kemenkopohukam, Kemendagri, TNI, BSSN, BIN, dan Kemenlu. Namun, perkuatan dari sisi manusia/SDM Indonesia juga tidak kalah penting untuk memperkuat ketahanan siber dan menekan dampak kerugian ekonomi yang dapat mengancam stabilitas negara seiring semakin terintegrasinya teknologi dalam berbagai aktivitas warga negara, termasuk aktivitas ekonomi. Program penguatan ketahanan digital Indonesia melalui SDMnya belum ada program khusus. Saat ini tercatat di RKP 2022, terdapat program literasi digital di Kementerian Komunikasi dan Informatika, namun cakupannya masih terbatas dan belum menyeluruh.

Dalam penanganannya, kejahatan siber ditangani secara silo dan cenderung reaktif. Kejahatan siber yang menyerang berbagai domain, mulai dari keuangan hingga pertahanan, perlu diatasi secara terkoordinasi, melibatkan berbagai stakeholder lintas sektor, dan terencana dari pencegahan hingga penanggulangan.

3. Saran dan Rekomendasi

Sejalan dengan dinamika perkembangan teknologi kedepan yang akan semakin dipenuhi disrupsi dan inovasi sehingga kehidupan manusia akan semakin bergantung pada teknologi informasi, penanganan kejahatan siber sudah sepatutnya dilakukan secara menyeluruh, preventif hingga kuratif, dan juga lintas sektor. Oleh karena itu terdapat beberapa masukan yang dapat dipertimbangkan oleh Komisi III DPR RI, diantaranya yaitu:

1. Komisi III dapat mendorong Polri selaku institusi penegakkan hukum agar dapat berkolaborasi dengan Kominfo untuk mendorong program peningkatan literasi digital, diantaranya melalui sosialisasi agar kesadaran menggunakan teknologi digital dengan aman masyarakat meningkat. Pemanfaatan teknologi digital yang aman diharapkan dapat menekan kerugian dan korban dari kejahatan siber.
2. Komisi III berkolaborasi dengan berbagai Komisi sektoral terkait dapat mendorong perkuatan koordinasi lintas lembaga untuk memperkuat pencegahan tindak kejahatan siber melalui perumusan kebijakan yang bersifat holistik dan pembagian peran masing – masing kementerian/lembaga yang jelas.
3. Regulasi yang mengakomodasi mengenai kejahatan siber saat ini dipandang belum cukup, dikarenakan UU ITE bertumpu pada konten (Thomas, 2019). Diperlukan kolaborasi lintas komisi untuk memperkuat regulasi terkait pencegahan dan penanganan kejahatan siber.

DAFTAR PUSTAKA

- Annur, C. M. (2022, 03 23). *Ada 204.7 juta pengguna internet di Indonesia awal 2022*. Retrieved from Databoks: <https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022>
- CNN Indonesia. (2022, July 1). *RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan*. Retrieved from CNN Indonesia: <https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan>
- Colleen McClain, E. A. (2021, September 1). *The Internet and Pandemic*. Retrieved from Pew Research Centre: <https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/>
- Harsono, N. (2022, January 20). *Despite Improvements, Indonesia's digital literacy remains low*. Retrieved from The Jakarta Post: <https://www.thejakartapost.com/business/2022/01/20/despite-improvements-indonesias-digital-literacy-remains-low.html>
- Hidayat, F. (2021, August 7). *Belanja Daring Meningkatkan saat Pandemi, Tokopedia Terbanyak Dikunjungi*. Retrieved from Berita Satu: <https://www.beritasatu.com/ekonomi/810987/belanja-daring-meningkat-saat-pandemi-tokopedia-terbanyak-dikunjungi>
- Interpol. (2021). *ASEAN Cyberthreat Assesment 2021*. Singapore: Interpol.
- Kantrowitz, M. (2021, January 1). *Permanent Changes Due To The Pandemic*. Retrieved from Forbes: <https://www.forbes.com/sites/markkantrowitz/2021/01/01/permanent-changes-due-to-the-pandemic/?sh=6dfbb30626aa>
- Nurhayati-Wolff, H. (2021, May 2020). *Internet Usage in Indonesia - statistics & facts*. Retrieved from Statista: https://www.statista.com/topics/2431/internet-usage-in-indonesia/#topicHeader__wrapper
- Nursyamsi, M. (2021, July 31). *Telkom: Trafik Data Internet Naik Selama PPKM Darurat*. Retrieved from Republika.id: <https://republika.id/posts/18986/telkom-trafik-data-internet-naik-selama-ppkm-darurat>
- Prahassacitta, V. (2019, 06 03). *Konsep Kejahatan Siber dalam Sistem Hukum Indonesia*. Retrieved from Binus University Business Law: <https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/>
- Rhani, A. R. (2020, October 08). *5 Manfaat Internet*. Retrieved from Kompas.com: <https://www.kompas.com/skola/read/2020/10/08/224859069/5-manfaat-internet?page=all>
- Thomas, V. F. (2019, February 9). *UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber*. Retrieved from Tirto.id: <https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU>