ISO 9001:2015
Certificate No. IR/QMS/00138

ANALISIS RUU TENTANG APBN

No. 13/an.PKA/APBN/IX/2021

Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan

PUSAT KAJIAN ANGGARAN
BADAN KEAHLIAN - SEKRETARIAT JENDERAL
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA

RINGKASAN EKSEKUTIF

TANTANGAN PENGUATAN KEAMANAN SIBER DALAM MENJAGA STABILITAS KEAMANAN NASIONAL

Ratna Christianingrum & Ade Nurul Aida

Saat ini Teknologi Informasi Dan Komunikasi (TIK) menjadi bagian tak terpisahkan dari segala aspek kehidupan masyarakat, baik dalam aspek kehidupan. Pertumbuhan TIK di Indonesia berkembang cukup pesat, terutama terkait penggunaan internet. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) periode 2019-kuartal 1/2020, bahwa jumlah pengguna internet di Indonesia mencapai 196,7 juta jiwa, atau sebesar 73,7% hingga kuartal II 2020. Namun peningkatan penggunaan internet juga meningkatkan ancaman keamanan siber. Peningkatan lalu lintas internet telah menarik pelaku-pelaku kriminal siber dan berakibat pada banyaknya kasus serangan siber di Indonesia. BSSN mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Bareskrim juga menyampaikan adanya peningkatan laporan kejahatan siber. Dimana Pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patrolisiber meningkat dari tahun sebelumnya 4.360 laporan pada 2018 (Patrolisiber, 2020). Sejalan dengan hal tersebut keamanan siber menjadi isu prioritas di Indonesia. Untuk itu tulisan ini akan membahas bagaimana kondisi keamanan siber di Indonesia, maupun tantangan dalam penguatan keamanan siber itu sendiri.

Dalam upaya meminimalisir dan mengatasi ancaman siber diperlukan penguatan keamanan siber, dimana tingkat urgensi keamanan siber berbanding lurus dengan tingkat ketergantungan pemanfaatan di ruang siber. Pengamanan ruang siber di Indonesia masih menghadapi beberapa tantangan, antara lain minimnya dukungan anggaran, rendahnya kesadaran masyarakat akan keamanan siber, belum adanya regulasi dan kebijakan bagi keamanan siber, minimnya kompetensi SDM, terbatasnya pengembangan teknologi keamanan siber domestik, serta belum adanya regulasi yang mengatur tentang penanganan tindak pidana siber.

Guna meningkatkan keamanan siber di Indonesia, maka perlu adanya: Pertama, Dukungan melalui peningkatan anggaran dibutuhkan dalam upaya penguatan keamanan siber dan penanganan tindak pidana siber. Kedua, edukasi keamanan siber sejak dini guna membangun kesadaran keamanan dari pengguna internet atau ruang siber. Ketiga, percepatan pengaturan regulasi sehubungan dengan keamanan siber. Keempat, perlunya dukungan dari Universitas dalam melahirkan SDM yang unggul dan berkompetensi khususnya dalam bidang siber. Kelima, perlu adanya insentif bagi start up dalam bidang keamanan siber sebagai upaya mendorong lahirnya perangkat teknologi dalam negeri. Keenam, sinergitas antar Kepolisian dan Kominfo perlu ditingkatkan guna menangani tindak pidana siber yang terus mengalami peningkatan.

TANTANGAN PENGUATAN KEAMANAN SIBER DALAM MENJAGA STABILITAS KEAMANAN NASIONAL

Ratna Christianingrum & Ade Nurul Aida

Pendahuluan

Saat ini Teknologi Informasi Dan Komunikasi (TIK) menjadi bagian tak terpisahkan dari segala aspek kehidupan masyarakat, baik dalam aspek ekonomi, sosial, budaya, pendidikan, kesehatan, dll. Pertumbuhan TIK di Indonesia sendiri berkembang cukup pesat terutama terkait penggunaan internet. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) periode 2019-kuartal 1/2020, bahwa jumlah pengguna internet di Indonesia mencapai 196,7 juta jiwa, atau sebesar 73,7% hingga kuartal II 2020. Angka tersebut naik 64,8% jika dibandingkan 2018. Di satu sisi, peningkatan pengguna internet ini merupakan merupakan berita baik atas meningkatnya kapabilitas masyarakat dalam beradaptasi dengan perkembangan teknologi, namun di sisi lain ancaman keamanan siber pun juga turut semakin meningkat.

Peningkatan lalu lintas internet telah menarik pelaku-pelaku kriminal siber dan berakibat pada banyaknya kasus serangan siber di Indonesia. Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Dimana pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patrolisiber (laman web Bareskrim untuk melaporkan kejahatan siber) meningkat dari tahun sebelumnya 4.360 laporan pada 2018 (Patrolisiber, 2020).

Dengan memperhatikan hal tersebut, ruang siber perlu mendapatkan perlindungan yang layak guna menghindari potensi yang dapat merugikan pribadi, organisasi bahkan negara. Sejalan dengan hal tersebut keamanan siber menjadi isu prioritas di berbagai negara termasuk Indonesia. Indonesia telah menetapkan keamanan siber menjadi prioritas nasional sebagaimana termuat dalam agenda pembangunan Rencana Pembangunan Jangka Menengah Nasional (RPJMN) IV tahun 2020–2024 dalam Prioritas Nasional (PN) 7, yakni memperkuat stabilitas politik, hukum, pertahanan, keamanan (polhukhankam), maupun Program Prioritas (PP) 5 dalam Rencana Kerja Pemerintah (RKP) tahun 2022[1].

[1] Fokus penekanan pada bidang pertahanan dan keamanan sebagaimana tertuang dalam PP 5, antara lain (1) pembangunan gelar kekuatan TNI; (2) pembangunan kemandirian industri pertahanan; (3) peningkatan keamanan laut; (4) peningkatan pelayanan kepolisian yang Prediktif, Responsibilitas, dan Transparansi Berkeadilan (PRESISI) berbasis digital; (5) peningkatan resiliensi masyarakat, terutama remaja dalam mencegah penyalahgunaan narkotika; (6) peningkatan pencegahan penyebaran ekstremisme dan radikalisme melalui sarana digital; dan (7) penguatan ketahanan dan keamanan siber. (Kementerian PPN/Bappenas, 2021)

Ancaman terhadap ruang siber sendiri merupakan konsekuensi logis dari berkembangnya era teknologi informasi dan komunikasi. Penguatan keamanan siber merupakan sebuah keniscayaan dan menjadi suatu kewajiban prioritas bagi negara dan semua instansi di dalamnya sebagai bagian dalam mewujudkan keamanan nasional, dimana tingkat urgensi keamanan siber berbanding lurus dengan tingkat ketergantungan pemanfaatan di ruang siber tersebut. Untuk itu tulisan ini akan membahas bagaimana kondisi keamanan siber di Indonesia, maupun tantangan dalam penguatan keamanan siber itu sendiri.

Kondisi Ancaman dan Keamanan Siber di Indonesia

Serangan siber merupakan serangan pada sistem komputer atau jaringan komputer untuk mendapatkan kendali atau akses tanpa izin ke sistem komputer yang ditargetkan (Maurer & Morgus, 2014; Marshall & Saulawa, 2015). Sementara kejahatan siber adalah aktivitas ilegal yang menggunakan dan menargetkan sistem atau jaringan komputer (ITU, 2012) Dalam definisi lain, kejahatan siber adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan (Abidin, 2017) yang menimbulkan kerugian materiil atau immateriil pada pihak yang menjadi target (Wilson, 2008). Kejahatan siber atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi (Saragih & Azis, 2020).

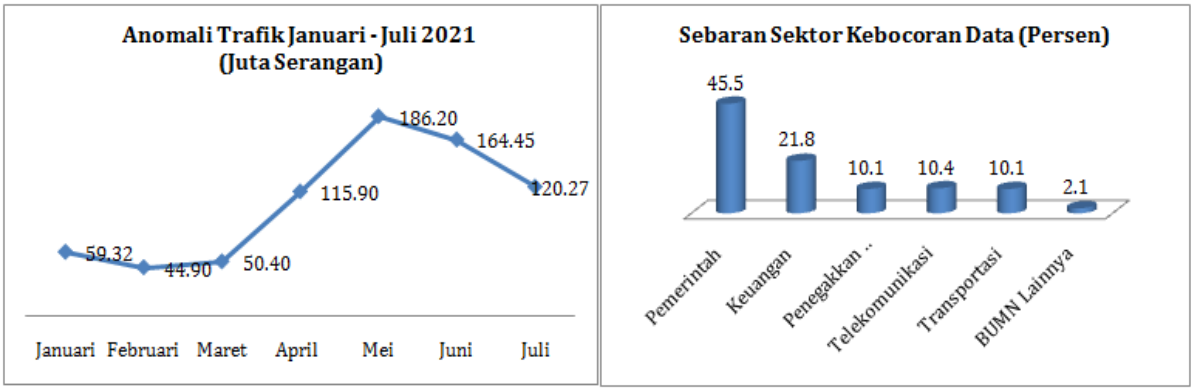
Pada dasarnya tidak semua serangan siber diartikan sebagai kejahatan, namun baik serangan siber maupun kejahatan siber dianggap sebagai ancaman siber. Ancaman siber sendiri merupakan tindakan yang mungkin muncul dan berpotensi menyebabkan masalah serius terhadap jaringan atau sistem komputer dan berdampak dalam segala aspek (CIPS, 2019).

Berdasarkan laporan data anomali trafik BSSN (2021), sepanjang tahun 2020, Indonesia mengalami serangan siber mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Anomali trafik tertinggi terjadi pada tanggal 10 desember 2020 dengan jumlah mencapai 7.311.606 anomali. Trojan menjadi anomali dengan jumlah tertinggi. Amerika serikat merupakan negara sumber anomali dengan jumlah serangan tertinggi selama tahun 2020. Dan Indonesia juga merupakan negara dengan serangan tertinggi yang menjadi tujuan dari anomali yang berasal dari negara Indonesia sendiri (dengan alamat IP Indonesia). Dari laporan tersebut juga dideteksi terjadinya email *phishing* sebanyak 2.549 kasus dengan peningkatan jumlah kasus email *phishing* terjadi di bulan Maret - Mei 2020, 79.439 akun

yang mengalami data *breach*[2], dan sebanyak 9.749 mengalami *web defacement* dimana sektor akademik menjadi sektor dengan kasus terbanyak pada tahun 2020.

Sementara pada Januari hingga Juli 2021 *anomaly traffic*/serangan siber telah mencapai 741,4 juta, dimana kategori anomali terbanyak yakni *malware, denial of service* (mengganggu ketersediaan layanan), dan *trojan activity;* dan tren serangan siber yang terjadi didominasi oleh serangan *ransomware* (*malware* yang meminta tebusan) dan *indeks data leaks* (kebocoran data). Dalam periode tersebut, sektor pemerintah merupakan sektor tertinggi yang mengalami kebocoran data akibat *malware* pencuri informasi yakni dengan sebaran 45,5%, yang kemudian disusul oleh sektor keuangan (21,8%), telekomunikasi (10,4%), penegakan hukum (10,1%), transportasi (10,1%), dan BUMN lainnya (2,1%).

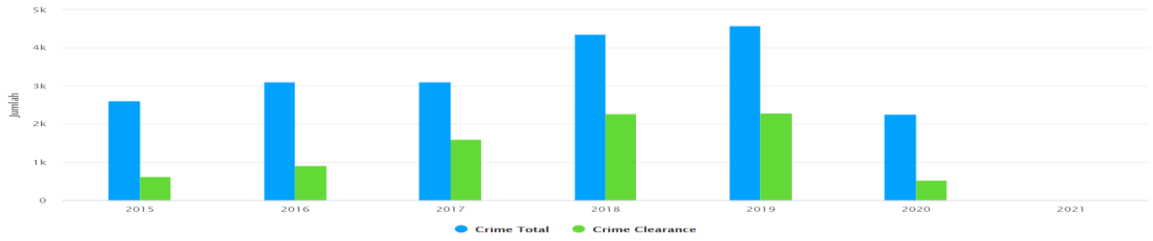
Gambar 1. Serangan Siber pada Januari Hingga Juli 2021



Sumber: BSSN, 2021

Bareskrim juga melihat adanya peningkatan laporan kejahatan siber. Dimana selama periode 2015 hingga 2019, kejahatan siber di Indonesia mengalami tren peningkatan (gambar 2). Namun pada tahun 2020, terjadi penurunan pengaduan kejahatan siber di Indonesia.

Gambar 2. Tren Kejahatan Siber Se-Indonesia



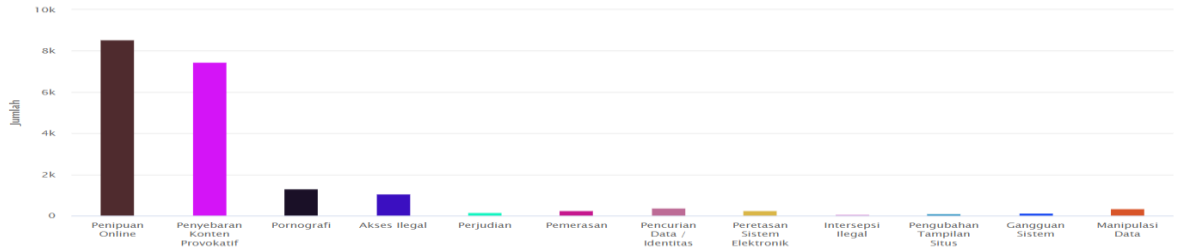
Sumber: Patrolisiber, 2020

Dalam kurung waktu 6 tahun terakhir, telah terdapat 25.759 aduan masyarakat melalui portal Patrolisiber dengan total kerugian mencapai Rp5,05 triliun. Penipuan *online* merupakan jenis tindak pidana yang paling tinggi terjadi. Penipuan secara *online* yang dimaksud dalam *e-commerce* adalah penipuan secara *online* yang menggunakan

[2] Insiden *data breach* menjadi topik besar di Indonesia selama tahun 2020 sejak bocornya 91.000.000 data berupa identitas pengguna salah satu *e-commerce* terbesar di Indonesia, Tokopedia, bocor di internet, yang tidak lama kemudian disusul oleh kebocoran data 1,2 juta pengguna situs Bhinneka

internet untuk keperluan bisnis dan perdagangan sehingga tidak lagi mengandalkan basis perusahaan yang konvensional yang nyata (Paryadi, 2018). Total laporan penipuan *online* mencapai 8.541 kasus

Gambar 3. Jenis Tindak Pidana Siber di Indonesia



Sumber: Patrolisiber,2020

Tidak pidana siber di Indonesia terjadi dan menyebar di seluruh wilayah Indonesia. Provinsi Jawa Barat merupakan wilayah dengan tingkat tindak pidana siber tertinggi di Indonesia. Selama lima tahun terakhir, jumlah kasus tindak pidana siber yang dilaporkan mencapai 5.265 kasus. Sedangkan Sulawesi Barat merupakan provinsi dengan jumlah kasus terendah di Indonesia, yakni hanya sebesar 21 kasus.

Kerugian dari serangan siber dan kejahatan siber tergantung pada karakteristik korban. Bagi korban korporasi, serangan siber dan kejahatan siber menyebabkan kerugian ekonomi dalam bentuk berkurangnya laba, kerugian nilai pasar, tuntutan hukum, dan rusaknya reputasi. Bagi korban individu, kerugian dari serangan siber dan kejahatan siber menyebabkan dampak stres dan psikologis, pencurian identitas, dan kerugian finansial (Acquisti, Friedman, & Telang, 2006; Agrafiotis et al., 2018; Telang & Wattall, 2007;). Berdasarkan studi Frost & Sullivan yang dilakukan Microsoft (2018) menemukan bahwa tiga dari lima (60 persen) perusahaan di Asia Pasifik menunda transformasi digital karena kekhawatiran akan risiko dari serangan siber. Serangan siber dapat merugikan perusahaan besar rata-rata USD18,7 juta baik dalam kerugian ekonomi langsung dan tidak langsung. Sementara untuk perusahaan menengah, rata-rata kerugian ekonomi adalah USD47.000 per perusahaan. Bahkan hampir tiga dari empat (73 persen) serangan keamanan siber selama 1 tahun telah mengakibatkan hilangnya pekerjaan di berbagai sektor.

Pada tahun 2017 insiden keamanan siber di Indonesia menyebabkan kerugian ekonomi sekitar USD34,2 miliar atau Rp478,8 triliun (setara dengan 3,7 persen dari total GDP Indonesia sebesar USD932 miliar) (BSSN, 2021). Penghitungan tersebut termasuk kerugian yang bersifat: langsung – kerugian finansial dari kerugian produktivitas, denda, dan biaya perbaikan; tidak langsung – hilangnya kesempatan karena perusahaan harus membangun kembali hubungan dengan konsumen setelah reputasinya rusak; dan terinduksi – insiden keamanan siber memiliki dampak pada ekonomi dan ekosistem yang lebih luas sehingga menyebabkan penurunan jumlah konsumen dan pendapatan.

Dalam melindungi dan meminimalisir ruang siber dari ancaman siber maka diperlukan keamanan siber agar ruang siber dapat terus tetap berjalan. Keamanan siber terdiri dari praktik, tindakan-tindakan, dan upaya-upaya yang melindungi ekosistem

siber dan aset-aset perusahaan dan pengguna dari serangan berbahaya yang bertujuan untuk mengganggu kerahasiaan, integritas, dan ketersediaan informasi atau data (Fischer, 2005; ITU, 2012). Data Global Cybersecurity Index 2020 yang didasarkan atas konsep lima kategori penilaian atau dinamakan *The Five Pilars of GCI Framework* yaitu *legal, technical and procedure, organizational, capacity building, dan international cooperation,* menunjukkan bahwa posisi keamanan siber Indonesia berada pada peringkat 24 dengan skor 94,88, jauh berada dibawah negara Singapura maupun Malaysia yang berada pada posisi 4 dan 5.

Gambar 4. Peringkat Keamanan Siber di Dunia Tahun 2020

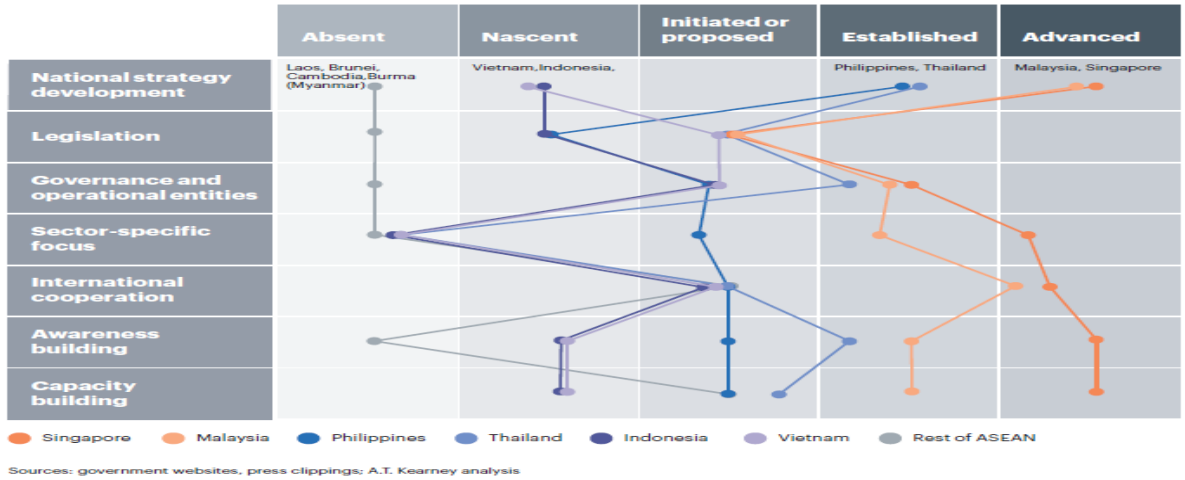
Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99,54	2
Saudi Arabia	99,54	2
Estonia	99,48	3
Korea (Rep. of)	98,52	4
Singapore	98,52	4
Spain	98,52	4
Russian Federation	98,06	5
United Arab Emirates	98,06	5
Malaysia	98,06	5
Lithuania	97,93	6
Japan	97,82	7
Canada**	97,67	8
France	97,6	9
India	97,5	10
Turkey	97,49	11
Australia	97,47	12
Luxembourg	97,41	13
Germany	97,41	13

Country Name	Score	Rank
Portugal	97,32	14
Latvia	97,28	15
Netherlands**	97,05	16
Norway**	96,89	17
Mauritius	96,89	17
Brazil	96,6	18
Belgium	96,25	19
Italy	96,13	20
Oman	96,04	21
Finland	95,78	22
Egypt	95,48	23
Indonesia	94,88	24
Viet Nam	94,59	25
Sweden	94,55	26
Qatar	94,5	27
Greece	93,98	28
Austria	93,89	29
Poland	93,86	30

Sumber: Global Cybersecurity Index 2020

Berdasarkan data A.T. Kearney (2018) sektor khusus keamanan siber di Indonesia masih sangat kurang bahkan masih belum hadir. Sementara baik dari sisi strategi nasional, peningkatan kesadaran, peningkatan kapasitas, maupun legislasi atau aturan perundang-undangan di Indonesia baru mulai terbentuk (Gambar 5).

Gambar 5. Posisi Keamanan Siber di Negara ASEAN

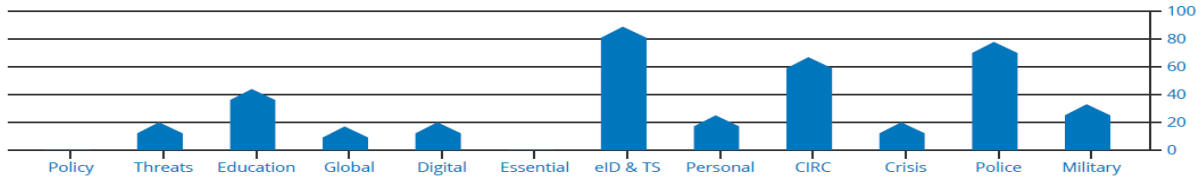


Sumber: A.T. Kearney, 2018

Tak berbeda dengan hasil data laporan Nasional Cyber Security Index (2021), yang menempatkan Indonesia pada urutan ke-5 dari 10 negara ASEAN dengan skor indeks

38,96 dan berada di urutan 77 dari 160 negara yang masuk dalam analisa NCSI tahun 2020. Dimana hasil laporan tersebut menyebutkan bahwa regulasi atau aturan perundang-undangan di Indonesia masih lemah disamping perlindungan layanan yang esensial dalam keamanan siber (gambar 6). Hal ini juga ditandai dengan dasar hukum yang mengatur keamanan siber di Indonesia hanya termuat dalam UU Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 yang kemudian direvisi menjadi UU ITE Nomor 19 Tahun 2016. UU ini mencakup aturan untuk beberapa pelanggaran, seperti mendistribusikan konten ilegal, pelanggaran perlindungan data, akses tidak berizin ke sistem komputer untuk mendapatkan informasi, dan sebuah pengambilalihan atau penyadapan ilegal dan tidak berizin terhadap sistem komputer atau elektronik lain.

Gambar 6. Persentase Pemenuhan Penilaian Analisa NCSI di Indonesia



Sumber: National Cybersecurity Index, 2021

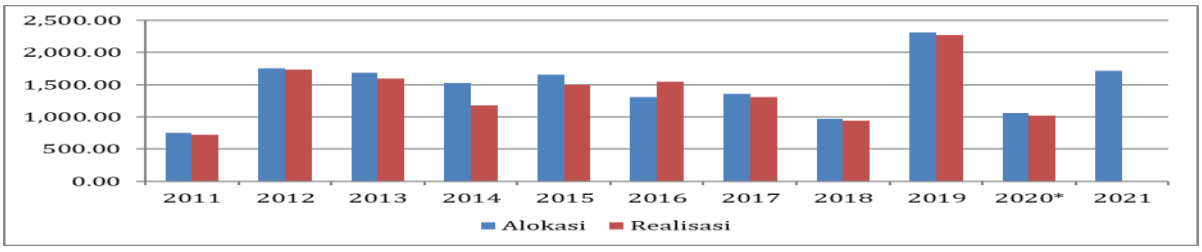
Tantangan Keamanan Siber

Dalam upaya meminimalisir dan mengatasi ancaman siber diperlukan penguatan keamanan siber, dimana tingkat urgensi keamanan siber berbanding lurus dengan tingkat ketergantungan pemanfaatan di ruang siber. Meski demikian pada praktiknya dalam upaya tersebut masih diliputi oleh sejumlah tantangan, sebagaimana berikut:

Minimnya Dukungan Anggaran

Maju dan canggihnya keamanan siber berkorelasi dengan belanja keamanan siber yang dikeluarkan (Qamar, 2020). Sepanjang tahun 2011 hinga 2021 anggaran pada lembaga BSSN, dimana merupakan lembaga yang memiliki tugas utama dalam bidang keamanan siber cenderung mengalami fluktuatif, dimana pada tahun 2019 merupakan kenaikan anggaran tertinggi sepanjang tahun tersebut.

Gambar 7. Anggaran Belanja BSSN Tahun 2011-2021 (Rp miliar)

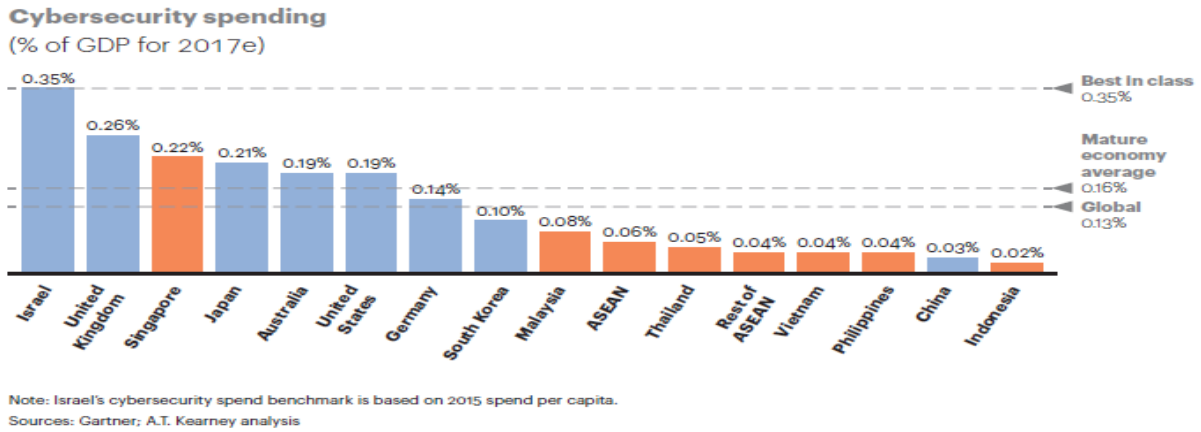


*Realisasi berdasarkan data Laporan Kinerja BSSN Tahun 2020
Sumber: LKPP berbagai Tahun, Nota Keuangan 2021, Laporan Kinerja BSSN Tahun 2020

Namun sayangnya dukungan belanja keamanan siber di Indonesia sendiri masih relatif kecil. 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. Hal ini menunjukkan bahwa dukung anggaran keamanan siber oleh pemerintah masih sangat terbatas.

Gambar 8. Rasio Belanja Keamanan Siber terhadap GDP (Persen)



Sumber: A.T. Kearney, 2018

Anggaran penindakan tidak pidana siber di Kepolisian mencapai Rp43,53 miliar pada tahun 2020, dimana penanganan tindak pidana siber merupakan salah satu tugas dan tanggungjawab Kepolisian RI. Anggaran ini digunakan untuk mewujudkan stabilitas politik dan keamanan melalui penegakan hukum yang professional, proporsional, dan akuntabel serta menjunjung tinggi hak asasi manusia khususnya dalam keamanan siber (Kepolisian RI, 2020). Namun apabila dilakukan perbandingan antara anggaran penindakan tindak pidana siber tersebut dengan jumlah kasus tindak pidana siber yang sebesar 12.197 di tahun yang sama, maka diperoleh bahwa anggaran penanganan kasus kejahatan siber rata-rata sebesar Rp3,57 juta. Nilai ini jauh dari kata ideal, mengingat anggaran tindak pidana umum dengan indikator kinerja perkara mudah di tingkat POLSEK memerlukan anggaran sebesar Rp 5 juta per kasus (Kepolisian Resot Sumbawa, 2019). Sedangkan untuk penanganan kasus tindak pidana umum dengan indikator kinerja perkara sedang di tingkat POLSEK memerlukan anggaran sebesar Rp15 juta per kasus (Kepolisian Resot Sumbawa, 2019). Sedangkan anggaran penyidikan taktis inteligen di lingkungan Baintelkam Mabes Polri, besaran anggaran yang penyidikan mencapai Rp20 juta per kasus. Dalam proses penyidikan kasus-kasus tindak pidana siber metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika, terutama dalam *undercover* dan *control delivery*. Hal ini dapat diartikan bahwa penanganan tindak pidana siber memiliki kompleksitas yang lebih dibandingkan dengan tindak pidana umum. Hal ini menunjukkan bahwa dukungan anggaran bagi penindakan tindak pidana siber masih kurang. Minimnya dukungan anggaran tersebut dapat berakibat pada tidak tertanganinya laporan masyarakat atas tindak pidana siber yang terjadi, yang dalam jangka panjang juga berakibat pada menurunnya kepercayaan masyarakat terhadap aparat penegak hukum.

Rendahnya Kesadaran Masyarakat Akan Keamanan Siber

Kesadaran keamanan siber dimasyarakat masih tergolong rendah, selain didasarkan atas laporan A.T Kearney (2018) yang menjelaskan bahwa kesadaran masyarakat atas keamanan siber masih dalam kategori nascent (baru lahir/terbentuk) hal ini juga ditunjukkan berdasarkan penelitian yang telah dilakukan oleh Communication and Information System Security Research Center (CISSReC) (2017) pada sembilan kota besar tanah air (DKI Jakarta, Bandung, Semarang, Yogyakarta, Surabaya, Medan, Palembang, Bali dan Makasar), bahwa hanya sebanyak 33 persen masyarakat sadar akan pentingnya melakukan keamanan siber. Hal ini menunjukkan bahwa sebagian besar masyarakat masih enggan untuk melakukan pengamanan pada aset yang terkoneksi ke wilayah siber.

Kebijakan/ Regulasi yang Belum Sepenuhnya Mendukung

Indonesia sendiri, sejauh ini memang belum memiliki suatu *grand design* kebijakan keamanan siber yang komprehensif dan integratif untuk menghadapi berbagai ancaman siber yang ada (BSSN, 2020). Berdasarkan laporan BSA The Software Alliance (2015), Indonesia sedang dalam tahap awal mengembangkan strategi keamanan siber nasional. Kerangka hukum untuk keamanan siber di Indonesia masih tergolong lemah, bahkan tidak adanya undang-undang atau kebijakan keamanan rahasia yang jelas, dan praktik keamanan tersebar di berbagai undang-undang. Selain itu juga tidak terdapat ketentuan keamanan siber khusus yang berlaku.

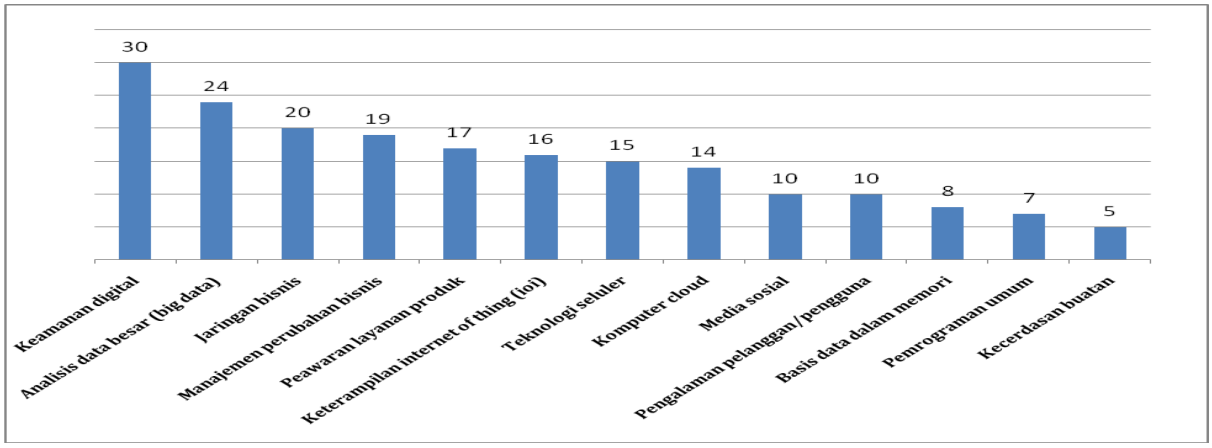
Regulasi yang ada saat ini hanya terkait Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), RUU tentang Perlindungan Data Pribadi pun masih dalam proses pembahasan oleh DPR, sementara RUU tentang Keamanan dan Ketahanan Siber juga belum ada pembahasan lebih lanjut. UU ITE sendiri memberikan perlindungan hukum untuk konten sistem elektronik dan transaksi elektronik. Akan tetapi, UU ini tidak mencakup aspek penting keamanan siber, seperti infrastruktur informasi dan jaringan, serta sumber daya manusia dengan keahlian di bidang keamanan siber (CIPS, 2019).

Minimnya Kompetensi SDM

Sumber daya 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. Berdasarkan laporan yang disampaikan oleh Telstra dan The Economist Intelligence Unit (EIU) (2017) menyatakan bahwa jumlah lulusan yang dicetak oleh lembaga Pendidikan berkualitas tinggi belum cukup dalam memenuhi

kebutuhan perusahaan lokal. Gambar 9 menunjukkan kemampuan yang paling dibutuhkan saat ini merupakan kemampuan digital terkait keamanan digital.

Gambar 9. Keterampilan Digital yang Diburu (Persen)



Sumber: EIU, 2017

Sejalan dengan tersebut, Selain perguruan tinggi sebagai lembaga pendidik dan cikal dari terbentuknya SDM berkompetensi yang masih memiliki gap dengan kebutuhan dunia kerja, kurikulum keamanan siber pada perguruan tinggi pun juga belum menjadi komponen penting dalam pembelajaran, bahkan baru diakui DIKTI dalam beberapa tahun terakhir (BSSN, 2020).

Terbatasnya Pengembangan Teknologi

Perangkat teknologi informasi yang digunakan hampir sebagian besar merupakan produk dari luar negeri. Belum ada *start up local* yang bergerak dalam bidang keamanan siber (BSSN, 2020). Hal ini menjadi tantangan tersendiri bagi pembangunan keamanan siber di Indonesia. Sebagai contoh, guna menciptakan stabilitas keamanan nasional dalam penguatan keamanan siber, salah satu upaya yang dilakukan oleh Kepolisian ialah mengembangkan intelijen media. Sistem intelijen media yang digunakan Polri saat ini mengumpulkan data dari pemberitaan 6000 media online (nasional, lokal, dan internasional dari 132 negara), 165 media cetak (nasional, lokal dari 10 provinsi hingga saat ini), 11 media televisi nasional, media sosial Twitter, Facebook, Instagram, dan Youtube (Herlambang, 2019). Dengan menggunakan teknologi AI (*Artificial Intellegence*) dalam intelijen media, diharapkan Kepolisian dapat mencegah *post truth* yang berpotensi untuk mengganggu stabilitas keamanan nasional. Terkait dengan hal tersebut sistem intelijen media yang digunakan oleh Kepolisian saat ini merupakan perangkat teknologi informasi yang dibeli dari luar negeri. Mengingat alat-alat yang digunakan oleh Kepolisian dalam menjaga keamanan nasional merupakan teknologi yang dikembangkan oleh pihak ketiga, terlebih lagi transfer teknologi yang dilakukan saat pembelian teknologi informasi, jarang diikuti dengan transfer *knowledge*. Tentunya hal ini menjadi satu kendala dalam upaya meningkatkan keamanan siber.

Sinergitas dalam Penanganan Tindak Pidana Siber

Penanganan tindak pidana siber di Indonesia dapat dilakukan oleh Kepolisian Republik Indonesia dan Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). Hal ini dimungkinkan terjadi, mengingat di Kominfo terdapat Penyidik Pegawai Negeri Sipil (PPNS) yang dapat membatu menyelidik dan memberikan bukti jejak digital dalam penanganan berbagai kasus kejahatan siber.

Namun tanpa adanya komunikasi dan sinergitas yang baik antara Kepolisian dan Kominfo, penangan tindak pidana siber di Indonesia dapat menjadi kurang optimal. Sehingga perlu adanya pembagian sektor yang jelas antara jenis tindak pidana siber yang akan dilakukan oleh Kepolisian atau Kominfo. Tanpa adanya pembagian sektor penanganan tindak pidana siber yang jelas, akan berakibat pada adanya beberapa sektor kasus tindak pidana siber yang akan ditangani oleh Kepolisian dan Kominfo. Hal ini dapat menimbulkan adanya konflik kepentingan antara kedua instansi tersebut. Namun di sisi lain, akan ada sektor tindak pidana siber yang tidak tertangani oleh kedua lembaga. Sehingga koordinasi dan sinergitas antara Kepolisian dan Kominfo dalam hal ini PPNS merupakan keharusan. Hal ini bertujuan agar tertanganinya tindak pidana siber yang terjadi di Indonesia secara optimal.

Penutup

Seiring berkembangnya era teknologi informasi dan komunikasi, keamanan siber menjadi hal yang sangat penting dan berbanding lurus dengan tingkat ketergantungan pemanfaatan di ruang siber. Penguatan keamanan siber merupakan sebuah keniscayaan dan menjadi suatu kewajiban prioritas bagi negara dan semua instansi didalamnya sebagai bagian dalam mewujudkan keamanan nasional. Namun dalam upaya tersebut masih diliputi oleh sejumlah tantangan. Upaya yang perlu pemerintah lakukan antara lain: **Pertama,** peningkatan dukungan anggaran guna meningkatkan keamanan siber maupun penanganan tindak pidana siber. **Kedua,** edukasi keamanan siber sejak dini, dalam hal ini bagaimana membangun kesadaran keamanan dari pengguna internet atau ruang siber. Setidaknya mitigasi pertama pengguna etika terjadi kebocoran data adalah mengubah kata sandi. Jika hal itu tidak dilakukan, dampak dan kerugiannya menjadi tidak terbatas. **Ketiga,** percepatan pengaturan regulasi sehubungan dengan keamanan siber. **Keempat,** perlunya dukungan dari Universitas dalam melahirkan SDM yang unggul dan berkompetensi khususnya dalam bidang siber. **Kelima,** perlu adanya insentif bagi *start up* dalam bidang keamanan siber sebagai upaya mendorong lahirnya perangkat teknologi dalam negeri. **Keenam,** sinergitas antar Kepolisian dan Kominfo perlu ditingkatkan guna menangani tindak pidana siber yang terus mengalami peningkatan.

Daftar Pustaka

Abidin, D. Z. (2017). Kejahatan dalam Teknologi Informasi dan Komunikasi. JurnalProcessor, 10(2), 509-516.

Acquisti, A., Telang, R., & Friedman A. (2006). Is there a cost to privacy breaches? An event study. Proceedings of the 3rd International Conferences on Intelligent System.

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding hot they propagate. Journal of Cybersecurity. Doi: 10.1093/cybsec/tyy006

BSA The Software Alliance. 2015. Asia Pacific Cyber Security Dashboard – A Path to a Secure Global; Cyberspace

BSSN. 2020. Renstra BSSN Tahun 2020-2024

BSSN. 2021. Laporan Tahunan: Monitoring Keamanan Siber 2020

CIPS. 2019. Ringkasan Kebijakan: Perlindungan Keamanan Siber di Indonesia

Frost & Sullivan. (2018). Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar. Diambil dari: https://news.microsoft.com/id-id/2018/05/24/

Herlambang, Rustika. (2019). Intelijen Media: Strategi, Prediksi, dan Antisipasi Potensi Kerawanan Kamtibmas 2020. Paparan dalam RAPIM POLRI 2019.

International Telecommunication Union. (2012). Understanding cybercrime: phenomena, challenges, and legal response. Diambil dari: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Kemenkominfo. 2018. Riset Kesadaran Keamanan Siber di Masyarakat Masih Rendah, diakses dari https://www.kominfo.go.id/content/detail/9992/, pada 26 Juli 2021

Kepolisian RI. (2020). Rencana Kinerja dan Anggaran Kepolisian RI.

Kepolisian Resot Sumbawa. (2019). Realisasi Anggaran Berjalan Reskrim Sumbawa.

Marshall, J., & Saulawa, M. (2015). Cyberattack: the legal response. International Journal of International Law, 1 (2). Diambil dari: http://www.ijoil.com/wp-content/uploads/2015/04/CYBER-ATTACKS-ACCEPTED-JOURNAL-1.pdf.

Maurer, T., & Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. New America Research Report.

Nasional Cyber Security Index, (2021). Diambil dari: https://ncsi.ega.ee/country/id/

Paryadi, D. (2018). Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen. Jurnal Hukum & Pembangunan, 48(3), 651-669.

Qamar, Adrian. 2020. Tantangan Keamanan Siber Bagi Industri & Bisnis di Era Indonesia. Disampaikan pada Acara Webinar Universitas Trisakti 12 Agustus 2020

Ramli, Kalamullah. 2020. Membangun Literasi Keamanan Siber: Tantangan Bagi Pemangku Kepentingan. Disampaikan pada Acara Webinar Universitas Trisakti 12 Agustus 2020

Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. Soumatera Law Review, 3(2), 265-279.

Telang, R., & Wattal S. (2007). An empirical analysis of the impact of software vulnerability announcement on firm stock price. IEEE Transactions on Software Engineering, 33. Doi: 10.1109/TSE.2007.70712

The Economist Intelligence Unit. (2017). Perdagangan Terhubung Kepercayaan Bisnis di Era Digital. Telstra.

Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress. Congressional Research Service

PUSAT KAJIAN ANGGARAN
BADAN KEAHLIAN SETJEN DPR RI
J. Jend. Gatot Subroto - Jakarta Pusat
Telp. (021) 5715635 - Fax (021) 5715635
http:// www.puskajianggaran.dpr.go.id

uskajianggaran
email: puskaji.anggaran@dpr.go.id