Jurnal Statistika dan Aplikasinya Volume 7 Issue 2, December 2023 e-ISSN: 2620-8369

Received: 27 October 2023
Revised: 22 December 2023
Accepted: 30 December 2023
Published: 31 December 2023

Determinan Kejahatan Siber (Cybercrime) di ASEAN Tahun 2015-2020: Pendekatan *Panel Data Regression with Random Effect*

Hafsha Daffa Dhiaulhaq[a)], Siskarossa Ika Oktora[b)]

Politeknik Statistika STIS

Email: [a)]hafsha.daffa@bps.go.id, [b)]siskarossa@stis.ac.id

Abstract

The use of information and communication technology in ASEAN is massive and growing. This development not only has a positive impact, but also a negative one. In addition to advancements in various fields, criminality is also increasing. ASEAN is the fastest growing digital market in the world. As digital technology becomes more integrated into our lives, cybercrime will increase exponentially. This study aims to determine the overview and variables that affect cybercrime in ASEAN in 2015-2020. This research uses secondary data from ITU, World Bank, UNDP, and Transparency International the Global Coalition Against Corruption. Through descriptive analysis, it is found that the value of the Global Cybersecurity Index (GCI) in ASEAN has increased, but there is still a cybersecurity gap between countries in ASEAN. Through the panel data regression equation formed, it is found that economic growth, mobile broadband users, and average years of schooling significantly affect the GCI in ASEAN in 2015-2020. Meanwhile, the variables of mobile cellular users, technology exports, and corruption perception index do not have a significant effect. Therefore, governments in ASEAN countries are also expected to continue to increase economic growth and allocate budgets for technical implementation of cybersecurity. In addition, the government should maintain the stability of the number of mobile broadband users, and increase the average number of mobile broadband users.

Kata-kata kunci: criminality, cybercrime, cyber security, panel regression

Abstrak

Penggunaan teknologi informasi dan komunikasi di ASEAN semakin masif dan terus berkembang. Perkembangan tersebut tidak hanya memberikan dampak positif, tetapi juga negatif. Selain kemajuan berbagai bidang, kriminalitas juga semakin meningkat. ASEAN merupakan pasar digital dengan pertumbuhan tercepat di dunia. Ketika teknologi digital semakin terintegrasi ke dalam kehidupan, cybercrime akan meningkat secara eksponensial. Penelitian ini bertujuan untuk mengetahui gambaran umum dan variabel yang memengaruhi cybercrime di ASEAN pada tahun 2015-2020. Penelitian ini menggunakan data sekunder dari ITU, World Bank, UNDP, dan Transparency International the Global Coalition Against

Corruption. Melalui analisis deskriptif didapatkan bahwa nilai Global Cybersecurity Index (GCI) di ASEAN mengalami kenaikan, tetapi masih terjadi kesenjangan keamanan siber antar negara di ASEAN. Metode yang digunakan dalam penelitian ini adalah regresi data panel dengan model *random effect model* (REM). *Random Effect Model* mengasumsikan bahwa setiap variabel mempunyai perbedaan intersep tetapi intersep tersebut bersifat random/stokastik. Model REM sesuai digunakan dalam menganalisis kejahatan siber karena mampu melihat pengaruh variabel secara *cross section* maupun *time series*. Melalui persamaan regresi data panel yang terbentuk didapatkan bahwa pertumbuhan ekonomi, pengguna mobile broadband, dan rata-rata lama sekolah signifikan memengaruhi GCI di ASEAN pada tahun 2015-2020. Sedangkan variabel pengguna mobile cellular, ekspor teknologi, dan indeks persepsi korupsi tidak berpengaruh secara signifikan. Oleh karena itu, pemerintah negara-negara di ASEAN juga diharapkan mampu terus meningkatkan pertumbuhan ekonomi dan mengalokasikan anggaran untuk pelaksanaan teknis keamanan siber. Selain itu, pemerintah sebaiknya menjaga stabilitas jumlah pengguna mobile broadband, dan meningkatkan rata-rata lama sekolah di masing-masing negara.

Kata-kata kunci: kriminalitas, *cybercrime*, *cyber security*, regresi data panel.

PENDAHULUAN

Teknologi informasi dan komunikasi atau *Information and Communication Technology* (ICT) berkembang secara pesat dari waktu ke waktu (Danuri et al., 2019). Salah satu kawasan yang terus mengalami perkembangan teknologi digital yaitu kawasan Asia khususnya *The Association of Southeast Asian Nations* (ASEAN) (Wicaksana, 2018). ASEAN termasuk pasar internet dengan pertumbuhan tercepat di dunia (Avirutha, 2021). Faktor digital menjadi salah satu faktor penting yang signifikan memengaruhi pertumbuhan ekonomi ASEAN secara positif (Wibowo, 2018). Selain itu, perkembangan ekonomi digital terus mengalami percepatan dan pembaharuan (Dwi Aprilia et al., 2021). Tidak hanya perekonomian, tetapi juga berbagai bidang lainnya telah mengalami fenomena digitalisasi (Reis et al., 2020). Transformasi berbagai bidang menuju media digital memerlukan keahlian dan keterampilan sebagai penyeimbang perubahan yang ada. Keterampilan ini sangat penting untuk mencapai tujuan *Sustainable Development Goals* (SDGs) (UN, 2021). Selain itu, literasi digital yang baik juga diperlukan dalam menghadapi era digital (Kusumastuti & Nuryani, 2019). Menurut UN (2020) penduduk yang belum memiliki kemampuan dan keterampilan teknologi digital tidak bisa merasakan manfaat dari kemajuan digital dan akan tertinggal jauh. Ketertinggalan terhadap teknologi digital yang ditandai dengan rendahnya literasi digital akan menyebabkan terjadinya *cybercrime* (Graham & Triplett, 2017). *Cybercrime* atau disebut dengan kejahatan di ruang siber adalah aktivitas kriminal di mana komputer atau jaringan komputer digunakan sebagai alat dan digunakan untuk melakukan aktivitas kriminal (Deora & Chudasama, 2021). Jenis-jenis kejahatan tersebut memiliki trend yang meningkat dan berdampak buruk bagi negara sasaran. Namun demikian, *cybercrime* masih belum mendapatkan perhatian, kepedulian, pencegahan dan pendidikan yang baik dan tepat (Viano, 2017).

ASEAN merupakan wilayah strategis dengan pertumbuhan Produk Domestik Bruto (PDB) potensial dan ekonomi digital yang terus meningkat. Kawasan ASEAN memiliki PDB gabungan lebih dari 3,11 triliun USD, sehingga menjadi salah satu dari pasar terbesar ketujuh di dunia. Wilayah ini berisiko menjadi sasaran *cybercrime* dan kehilangan miliaran dolar selama beberapa tahun ke depan jika tidak ada perbaikan yang dilakukan dalam struktur keamanan siber (Marmita, 2020). Para pelaku *cybercrime* tidak hanya merusak objek pemerintah atau infrastruktur nasional, tetapi juga telah membahayakan keamanan negara dan memiliki potensi *cyber warfare*, suatu bentuk ancaman yang sangat rentan terhadap pertahanan keamanan nasional (Maskun et al., 2021). Seluruh negara perlu melakukan tindakan untuk memberantas *cybercrime*. Salah satu alat yang dapat digunakan untuk mengetahui keparahan kejahatan siber suatu negara yaitu dengan melihat keamanannya (*cyber security)* melalui *Global Cybersecurity Index* (GCI) (Bruggemann et al., 2022).

Berdasarkan hasil laporan *ASEAN Cyberthreat Assessment 2021* kerugian akibat *cyberattacks* dan pembobolan data 3,86 juta USD, dan waktu rata-rata untuk mengidentifikasi dan memulihkannya adalah sekitar 280 hari. Penelitian yang dilakukan oleh Putri, K.V.K (2021) menunjukkan bahwa ASEAN telah melakukan berbagai kerjasama dan membuat peraturan perundang-undangan untuk menangani masalah *cybercrime*. Selain itu, ASEAN juga terus memperkuat keamanan siber di setiap negara. Namun, kerjasama serta aturan yang telah dibuat belum bekerja secara maksimal dalam menangani masalah kejahatan siber. Penelitian mengenai *cybercrime* di ASEAN belum banyak dikaji secara mendalam. Literatur kuantitatif mengenai *cybercrime* di ASEAN juga masih terbatas. Srivastava et al. (2020) melakukan penelitian kualitatif tentang faktor-faktor yang memengaruhi *cybercrime*. Penelitian ini menunjukkan bahwa kejahatan siber dipengaruhi oleh faktor kapabilitas teknologi, kapabilitas ekonomi, dan kesiapan yang mencakup hukum, kerjasama, teknis, pengembangan kapabilitas, dan organisasi dalam bidang siber. Selain itu, terdapat beberapa penelitian terkait kejahatan siber dan keamanan siber diantaranya Makridis & Smeets (2019), Solano et al. (2017), dan Tatarinovaa et al. (2016). Ketiga penelitian tersebut, tidak secara khusus meneliti *cybercrime* di ASEAN, melainkan beberapa negara lainnya. Melalui analisis regresi multivariat, Makridis & Smeets (2019) menemukan bahwa negara yang memiliki ketergantungan lebih besar terhadap dunia maya juga memiliki kesiapan siber yang lebih baik. Selain itu, dalam penelitiannya juga terdapat temuan bahwa PDB tidak signifikan memengaruhi kesiapan siber suatu negara.

Solano et al. (2017) dalam penelitiannya menemukan bahwa di Suriah terdapat korelasi positif antara faktor politik dan jumlah serangan siber. Selain itu, Solano et al. (2017) juga menemukan bahwa di Ghana terdapat korelasi kuat antara PDB dengan jumlah serangan siber. Berbeda dengan dua penelitian sebelumnya, penelitian yang dilakukan oleh Tatarinovaa et al. (2016) mengkaji faktor yang menyebabkan *cybercrime* secara kualitatif. Hasil penelitiannya menemukan bahwa kesenjangan pengetahuan tentang kriminologi di bidang siber dapat menjadi faktor pemicu munculnya kejahatan siber. Selain itu, terdapat penelitian yang telah dilakukan degan tujuan mengkaji terkait hukum dan Undang-undang (UU) mengenai *cybercrime*. Siregar & Sinaga (2021) menyebutkan bahwa regulasi *cybercrime* dalam UU mutlak diperlukan dan perlu membuat hukum tentang pelaku *cybercrime* yang berada dari lintas negara. Minimnya penelitian kuantitatif menyebabkan *cybercrime* hanya dicegah melalui perubahan-perubahan regulasi. Padahal pesatnya pertumbuhan kejahatan dunia maya mengharuskan pengembangan mekanisme yang efektif untuk mencegah kejahatan tersebut (Sviatun et al., 2021).

ASEAN masih memerlukan penelitian tentang *cybercrime* maupun *cyber security,* utamanya dengan pendekatan empiris kuantitatif. Penelitian yang masih sedikit mengenai kejahatan siber menyebabkan diperlukannya analisis yang lebih kompleks dengan melihat pengaruh tempat dan waktu. Oleh karena itu, analisis regresi data panel diperlukan untuk melihat pengaruh variabel independent terhadap variable dependen berdasarkan ruang dan waktu. Berdasarkan uraian sebelumnya, penelitian ini memiliki dua tujuan. Pertama, untuk mengetahui gambaran umum dari *Global Cybersecurity Index* yang terjadi di negara-negara ASEAN serta faktor yang diduga memengaruhinya. Kedua, untuk mengetahui faktor-faktor yang memengaruhi kejahatan siber (*cybercrime)* yang terjadi di negara-negara ASEAN.

METODOLOGI

Bahan dan Data Secara teoretis *cybercrime* termasuk tindak kriminalitas yang dapat disebabkan oleh beberapa faktor seperti ekonomi, pergaulan, dan kesempatan (Djanggih & Qamar, 2018). Dalam mengukur kesiapan siber guna mencegah terjadinya *cybercrime* di suatu negara, ITU membuat ukuran berupa indeks kemanan siber yang disebut dengan *Global Cybersecurity Index* (GCI). Selain sebagai ukuran, GCI juga dibuat untuk menumbuhkan budaya keamanan siber global. GCI pertama kali diluncurkan pada tahun 2015 oleh ITU untuk mengukur komitmen 193 Negara anggota ITU dan Palestina. GCI merupakan indeks komposit. GCI tersusun atas lima dimensi yang merupakan pilar dalam *Global Cybersecurity Agenda* (GCA) yaitu hukum, organisasi, kerjasama internasional, pengembangan kapabilitas, dan teknis.

Cybercrime di seluruh dunia sebagian besar tidak dilaporkan (UNODC, 2019). Rendahnya tingkat pelaporan membuat data frekuensi *cybercrime* kurang representatif untuk digunakan dalam penelitian. Dalam penelitian ini, tingkat *cybercrime* diukur menggunakan variabel GCI sebagai variabel dependen. Sedangkan untuk variabel independen terdiri dari variabel pertumbuhan ekonomi untuk melihat penyebab *cybercrime* dari dimensi ekonomi. Lalu untuk melihat penyebab *cybercrime* dari kapabilitas teknologi diwakili oleh variabel pengguna *mobile broadband* dan pengguna *mobile cellular*. Selain itu, aktivitas perdagangan dengan negara asing dan pendidikan juga diduga mampu memengaruhi GCI, pada penelitian ini diwakili oleh variabel ekspor teknologi dan Rata-rata Lama Sekolah (RLS). Variabel yang mengukur faktor *cybercrime* dari dimensi politik yaitu indeks persepsi korupsi. Variabel-variabel tersebut digunakan berdasarkan teori dari penelitian terdahulu dan ketersediaan data. Penelitian yang dilakukan oleh Solano et al. (2017) menyebutkan bahwa *cybercrime* dipengaruhi oleh faktor ekonomi, sosial, dan politik. Selain itu, penelitian yang dilakukan oleh Srivastava et al. (2020) menyebutkan bahwa selain faktor sosial ekonomi, faktor kapabilitas teknolgi juga memengaruhi terjadinya *cybercrime.* Data yang digunakan dalam penelitian ini merupakan data sekunder. Data tersebut bersumber dari laporan dan website ITU, *World Bank*, *United Nations Development Programme* (UNDP), dan *Transparency International the Global Coalition Against Corruption.* Ruang lingkup penelitian ini adalah seluruh negara anggota ASEAN yaitu Indonesia, Malaysia, Filipina, Singapura, Thailand, Brunei Darussalam, Vietnam, Laos, Myanmar, dan Kamboja. Penelitian ini menggunakan periode 2015-2020 sehingga terdapat 60 observasi penelitian. TABEL 1 menunjukkan data, simbol, satuan, sumber data, serta definisi operasional dari variabel yang digunakan dalam penelitian ini.

Data yang digunakan dalam penelitian ini merupakan data sekunder. Data tersebut bersumber dari laporan dan website ITU, Bank Dunia, United Nations Development Programme (UNDP), dan Transparency International the Global Coalition Against Corruption, dan SANS institute. Variabel dependen yang digunakan yaitu GCI. Variabel independen yang digunakan meliputi pertumbuhan ekonomi, pengguna mobile broadband, pengguna mobile cellular, persentase ekspor teknologi, rata-rata lama sekolah, dan indeks persepsi korupsi.

TABEL 1. Nama variabel, simbol dalam persamaan, definisi operasional, satuan, dan sumber data

No.	Nama Variabel	Simbol	Satuan	Definisi Operasional	Sumber
(1)	(2)	(3)	(4)	(5)	(6)
1.	Pertumbuhan ekonomi	PE	Persen	Perbandingan antara selisih PDB suatu negara pada tahun t dengan PDB suatu negara pada tahun t-1 dan PDB suatu negara pada tahun t-1	*World Bank*
2.	Pengguna *mobile broadband*	MB	Persen	Penggunaan layanan jaringan internet yang bersifat *wireless*, misalnya *smartphone* dan modem per 100 penduduk.	ITU
3.	Pengguna *mobile cellular*	MC	Persen	Pengguna layanan telepon seluler yang memiliki akses ke jaringan menggunakan teknologi seluler per 100 penduduk	ITU
4.	Ekspor teknologi	ET	Persen	Ekspor teknologi meliputi komputer dan peralatan periferal, peralatan komunikasi, peralatan elektronik konsumen, komponen elektronik, dan barang teknologi dan informasi lainnya (lain-lain).	*World Bank*
5.	Rata-rata lama sekolah	RLS	Tahun	Jumlah rata-rata tahun pendidikan yang diselesaikan dari penduduk suatu negara yang berusia 25 tahun ke atas, tidak termasuk tahun yang dihabiskan untuk mengulang kelas individu	UNDP
6.	Indeks persepsi korupsi	CPI	Poin atau angka	Suatu ukuran untuk mengukur persepsi masyarakat terhadap korupsi di negaranya. Semakin tinggi indeks ini, maka tingkat korupsi semakin rendah.	*Transparency International the Global Coalition Against*

					Corruption
7.	*Global Cybersecurity Index*	GCI	Poin atau angka	Ukuran keamanan siber suatu negara yang tersusun atas pilar hukum, Kerjasama internasional, teknis, pengembangan kapabilitas, dan organisasi.	ITU

Metode Penelitian

Dalam rangka menjawab tujuan penelitian, dilakukan analisis deskriptif dan analisis inferensia. Analisis deskriptif menggunakan grafik dan tabel, sedangkan analisis inferensia menggunakan regresi data panel. Berikut merupakan model yang akan dibentuk dalam penelitian ini:

$$GCI_{it} = \alpha + \beta_1 PE_{it} + \beta_2 MB_{it} + \beta_3 MC_{it} + \beta_4 ET_{it} + \beta_5 LnRLS_{it} + \beta_6 CPI_{it} + e_{it} \quad (1)$$

Keterangan:
Ln : logaritma natural
α : intersep
β_i : koefisien regresi variabel independent
e_{it} : komponen eror pada individu ke-i waktu ke-t
i : 1, 2, 3, …, 10
t : 1, 2, 3, …, 6

Adapun tahap-tahap dalam melakukan analisis regresi data panel adalah sebagai berikut:

1. Membentuk model regresi data panel *Common Effect Model* (CEM), *Fixed Effect Model* (FEM), dan *Random Effect Model* (REM).
2. Memilih model regresi data panel terbaik

a. Melakukan pengujian model dengan uji Chow

Hipotesis yang digunakan dalam uji Chow yaitu $H_0: \gamma_1 = \gamma_2 = \cdots = \gamma_9 = 0$ (Model CEM lebih baik). Pada tingkat signifikansi α, apabila uji Chow menghasilkan *p-value* $< 0{,}05$ keputusan yang didapatkan adalah tolak H_0, maka uji lanjutan yang perlu dilakukan adalah uji Hausman untuk memilih model terbaik antara FEM dan REM.

b. Melakukan pengujian model dengan uji Hausman

Hipotesis yang digunakan dalam uji Hausman adalah $H_0: E(v_i | X_{1it}, X_{2it}, \ldots, X_{6it}) = 0$ (eror tidak berkorelasi dengan variabel independent atau REM lebih baik) Untuk $i = 1, 2, 3, \ldots, 10,\ t = 2015, 2016, \ldots, 2020.$ Pada tingkat signifikansi α, apabila uji Hausman menghasilkan *p-value* < 0,05 keputusan yang didapatkan adalah tolak H_0, maka FEM lebih baik dibandingkan REM.

c. Melakukan pengujian model dengan BP-LM

Hipotesis yang digunakan dalam uji BP-LM adalah $H_0: \sigma_\gamma^2 = 0$ (model CEM lebih baik). Pada tingkat signifikansi α, apabila uji BP-LM menghasilkan *p-value*$< 0{,}05$ keputusan yang didapatkan adalah tolak H_0, maka REM lebih baik dibandingkan CEM. Apabila model yang terpilih adalah FEM atau CEM, maka perlu dilakukan pengujian struktur varians kovarians. Namun, apabila yang terpilih adalah REM maka estimasi yang akan digunakan adalah *Generalized Least Square* (GLS).

3. Pengujian struktur varians kovarians

a. Pengujian *Lagrange Multiplier* (LM).

Hipotesis yang digunakan dalam uji BP-LM adalah $H_0: \sigma_i^2 = \sigma^2$ (struktur varians kovarians bersifat homoskedastik). Apabila Uji LM ini menghasilkan keputusan gagal tolak H_0, maka dapat disimpulkan bahwa varians-kovarians dalam model bersifat homoskedastis. Sebaliknya, apabila keputusan yang dihasilkan adalah tolak H_0, artinya varians-kovarians dalam model bersifat heteroskedastis. Apabila hasil uji LM menghasilkan tolak H_0, maka perlu dilakukan pengujian λ_{LM}.

b. Uji λ_{LM}

Hipotesis yang digunakan dalam uji λ_{LM} adalah $H_0 : cov(\gamma_i, \gamma_j) = 0$ (tidak terdapat *cross-sectional correlation*). Apabila struktur varians-kovarians residual bersifat homoskedastis, maka estimasi yang tepat untuk digunakan yaitu *Ordinary Least Square* (OLS). Apabila struktur varians-kovarians residual bersifat heteroskedastis dan tidak ditemukan *cross sectional correlation* maka estimasi yang tepat digunakan yaitu *Weighted Least Square* (WLS). Jika struktur varians-kovarians residual bersifat heteroskedastis dan ditemukan adanya *cross sectional correlation* maka estimasi yang tepat digunakan yaitu *Feasible-Generalized Least Square-Seemingly Unrelated Regression* (FGLS-SUR).

4. Melakukan pengujian asumsi klasik

Setelah menentukan metode estimasi, maka dilakukan pengujian asumsi klasik. Pengujian asumsi klasik disesuaikan dengan metode estimasi yang digunakan. Apabila metode estimasi yang digunakan yaitu OLS, maka keempat asumsi klasik harus terpenuhi yaitu normalitas, homoskedastisitas, non-autokorelasi, dan non-multikolienaritas. Sementara itu, jika metode estimasi yang digunakan adalah *Generalized Least Square* (GLS) maka hanya dilakukan uji normalitas dan pemeriksaan non-multikolienaritas. Apabila asumsi klasik sudah terpenuhi, maka selanjutnya dilakukan pengujian keberartian model.

5. Keberartian Model

Dilakukan melalui pengecekkan nilai koefisien determinasi (R^2), uji simultan (uji statistik F), dan uji parsial (uji statistik t). Setelah didapatkan model yang fit, maka dilakukan interpretasi model yang diperoleh.

HASIL DAN PEMBAHASAN

GCI merupakan ukuran paling komprehensif yang mengukur lembaga pemerintah dan organisasi swasta tertentu dalam menciptakan sinergi yang diperlukan untuk mengatasi *cybercrime* (Farahbod et al., 2020). Selain itu, melalui GCI dapat diketahui kesenjangan keamanan siber berbagai negara di dunia.

Perkembangan nilai GCI dari tahun 2015 hingga 2020 di sepuluh negara ASEAN. GCI di Indonesia mengalami peningkatan yang cukup signifikan dari tahun 2015 hingga 2020, yakni dari 47,1 hingga 94,88. Meskipun pada tahun 2016 dan 2017 sempat mengalami tren menurun, tetapi kembali menunjukan kenaikan yang signifikan pada tahun 2018. Pada tahun 2019 GCI di Indonesia juga menunjukkan penurunan, namun kembali meningkat pada tahun 2020. Kenaikan nilai GCI di Indonesia merupakan hasil dari upaya kepolisian dan badan terkait yang terus mensosialisasikan mengenai bahaya kejahatan di dunia siber dan cara mencegahnya pada tahun 2020. Nilai keamanan siber di Indonesia rendah pada tahun 2015 sampai 2017 dikarenakan rendahnya kesadaran masyarakat mengenai keamanan siber. Hal tersebut disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis *cybercrime* (Nugraha, 2021). *Lack of information* menjadi kendala dalam penegakan hukum *cybercrime*, dalam hal ini kendala berkenaan dengan penaatan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cybercrime*.

GCI di Malaysia cenderung menunjukkan angka yang stabil dan tinggi. Pada tahun 2015 GCI Malaysia mencapai 76,5 dan mengalami peningkatan pada tahun 2020 menjadi sebesar 98,06. Dalam

hal pengembangan kapabilitas, Malaysia memiliki program pelatihan keterampilan teknis dan kompetensi serta sertifikasi profesi yang melibatkan domain cybersecurity. Selain itu, Malaysia mampu menghasilkan profesional *cybersecurity* tidak hanya secara internal tetapi juga dari luar negeri melalui Skema Sertifikasi ACE Global dan kolaborasi dengan sektor publik dan swasta, industri dan lembaga pendidikan tinggi. Melalui *Malaysian Technical Cooperation Programme* (MTCP), negara tersebut terakreditasi untuk melatih peserta dari negara-negara ASEAN dan juga Organisasi Kerjasama Islam (OKI). Malaysia juga aktif memperkuat kemitraan untuk memerangi terorisme siber di tingkat global melalui berbagai platform internasional, antara lain *Asean Computer Emergency Response Team* (ASEAN CERT), *Asean Regional Forum* (ARF), dan *Council for Security Cooperation in the Asia Pasifik* (CSCAP). Kementerian Komunikasi dan Multimedia (2021) menyampaikan bahwa bersama *cyber security* Malaysia tetap berkomitmen untuk terus memberdayakan dan menjaga infrastruktur dan ekosistem *cyber security* agar tetap kompetitif guna mencapai cita-cita membawa Malaysia ke era digitalisasi dan menjadi pelopor regional dalam ekonomi digital.

GCI Singapura merupakan indeks dengan nilai tertinggi dari sepuluh negara ASEAN. Nilai GCI di Singapura naik dari tahun 2015 sebesar 67,65 menjadi 98,52 pada tahun 2020. Tingginya nilai GCI di Singapura merupakan hasil kerjasama pemerintahan Singapura dengan beberapa badan yang berwenang. Sejak tahun 2016 Singapura telah meyusun strategi keamanan siber dan melakukan pembaharuan pada tahun 2021 (*Cyber Security Agency of Singapore*, 2021). Strategi keamanan siber yang dilakukan adalah membangun infrastruktur yang tangguh, menciptakan dunia maya yang lebih aman, mengembangkan ekosistem *cybersecurity* yang hidup, dan memperkuat kemitraan internasional (*Cyber Security Agency of Singapore*, 2016). Dalam keempat pilar tersebut, Singapura telah menyusun program sebagai bentuk realisasi strategi yang telah dibuat. Misalnya dengan memperluas dan memperkuat sumber daya nasional yaitu *National Cyber Incident Response Team* (NCIRT) dan the *National Cyber Security Centre* (NCSC).

GCI Thailand merupakan GCI tertinggi ketiga setelah Singapura dan Malaysia. Nilai GCI di Thailand menunjukkan kenaikan dari tahun ke tahun. Pada tahun 2015 GCI di Thailand bernilai 41,2 dan meningkat menjadi 86,5 pada tahun 2020. GCI Thailand sempat mengalami penurunan pada tahun 2019. Dari indeks yang bernilai 79,6 pada tahun 2018 menjadi 78,52 pada tahun 2019. Salah satu kendala yang dihadapi Thailand yaitu organisasi yang bertanggung jawab atas keamanan siber tidak memiliki regulasi keamanan siber (Charoen, 2018). GCI Brunei Darussalam juga mengalami kenaikan pada tahun 2020 jika dibandingkan tahun 2015. GCI pada tahun 2015 yaitu sebesar 38,2 menjadi 56,07 pada tahun 2020. Nilai GCI Brunei Darussalam sempat naik pada tahun 2018, namun dua tahun setelahnya mengalami penurunan. Angka kejahatan siber di Brunei Darussalam diketahui meningkat, tetapi keamanan siber semakin mengkhawatirkan (Chuchu & Abd Gafur, 2020). Meskipun demikian, Brunei Darussalam telah memiliki badan yang menangani *cybercrime* dan sudah cukup lama terbentuk, diantaranya himpunan yang terdiri dari beberapa lembaga seperti *IT Protective Security Service* (ITPSS) yang didirikan pada tahun 2003 dengan tujuan untuk menyediakan acuan untuk menyelamatkan informasi, *Digital Forensics, Secure Event Management, IT Security Training*, serta *Incident Response Team* yang didirikan pada tahun 2004 dengan nama *Brunei Computer Emergency Response Team* (BruCERT).

Perkembangan GCI Vietnam cenderung fluktuatif. Penurunan yang cukup signifikan terjadi pada tahun 2017. Sementara kenaikan paling signifikan terjadi pada tahun 2020. Pada tahun 2019 GCI Vietnam masih pada angka 65,6 dan naik pada tahun 2020 menjadi 94,59. Perubahan yang signifikan pada tahun 2020 ini disebabkan adanya upaya yang dilakukan oleh pemerintah Vietnam secara berkelanjutan. Pada tahun 2018 GCI Vietnam meningkat karena pemerintahan Vietnam merilis Undang-Undang terkait keamanan siber (Nguyen, 2018). GCI kembali menurun pada 2019 dan diindikasikan sebagai dampak dari kritik masyarakat. Undang-Undang Keamanan Siber Vietnam yang baru memberikan kekuatan baru yang luas kepada otoritas Vietnam dan memungkinkannya untuk memaksa perusahaan teknologi menyerahkan sejumlah besar data, termasuk informasi pribadi, dan untuk menyensor postingan pengguna (Algar, 2018).

GCI Filipina menunjukkan tren yang terus meningkat sejak tahun 2015 yaitu sebesar 35,3 hingga tahun 2020 yaitu sebesar 77. Namun, pada tahun 2019 GCI di Filipina mengalami penurunan menjadi sebesar 56,92. Sementara itu, nilai GCI 3 negara lainnya yaitu Laos, Myanmar, dan Kamboja

merupakan nilai GCI tiga terendah di ASEAN. GCI Laos tertinggi terjadi pada tahun 2017 yaitu sebesar 39,2, tetapi kembali mengalami penurunan pada tahun-tahun berikutnya. Nilai GCI Myanmar sangat fluktuatif dan tergolong rendah. GCI tersebut mengalami penurunan pada tahun 2016 dan 2018. Pada tahun 2016 GCI menjadi 11,39 yang semula sebesar 38,2 pada tahun 2015. Pada tahun 2018 nilainya menjadi 17,2 yang semula sebesar 25,31 pada tahun 2017. GCI tertinggi di Myanmar terjadi pada tahun 2015, dan terus menurun di tahun 2020. Nilai GCI di Kamboja tidak stabil, namun secara perlahan mengalami kenaikan. Nilai GCI tertinggi terjadi pada tahun 2017 yaitu sebesar 28,3.

Analisis Regresi Data Panel

Model regresi data panel memiliki tiga jenis model yaitu FEM, CEM, Dan REM. Dalam menentukan model terbaik diperlukan uji statistik yaitu uji Chow dan uji Hausman. Uji Chow dilakukan untuk memilih antara CEM dan FEM. Berdasarkan hasil uji Chow, nilai *Chi-square statistic* yang didapat yaitu 23,976 dengan *p-value* sebesar 0,0043. Dengan tingkat signifikansi 5% keputusan yang diperoleh adalah tolak H_0. Model yang lebih baik digunakan yaitu FEM dibandingkan dengan CEM. Oleh karena model yang lebih baik digunakan yaitu FEM, maka perlu dilakukan uji statistik selanjutnya yaitu uji Hausman. Uji Hausman dilakukan untuk memilih model yang lebih baik antara FEM dan REM. Berdasarkan hasil uji Hausman, didapatkan nilai *chi-square statistic* sebesar 3,167 dengan *p-value* sebesar 0,787. Dengan tingkat signifikansi 5% diperoleh keputusan gagal tolak H_0. Model yang lebih baik digunakan yaitu model REM dibandingkan FEM. Berdasarkan uji statistik yang telah dilakukan sebelumnya diperoleh hasil model terbaik yaitu REM. Uji tersebut didukung dengan teori bahwa REM lebih baik digunakan pada data panel apabila jumlah individu lebih besar daripada jumlah kurun waktu yang ada (Gujarati dan Porter, 2012: 602). Selanjutnya, sesuai dengan metode estimasi dan model terbaik yang digunakan pada penelitian ini, maka akan dilakukan pengujian normalitas dan pemeriksaan multikolienaritas.

Pengujian normalitas pada penelitian ini menggunakan uji statistik Jarque-Bera. Berdasarkan hasil uji normalitas didapatkan nilai statistik sebesar 1,256 dengan *p-value* 0,354. Hasil tersebut menunjukkan bahwa dengan tingkat signifikansi 5% diperoleh keputusan gagal tolak H_0. Oleh karena itu, dapat disimpulkan bahwa eror berdistribusi normal atau asumsi normalitas terpenuhi. Pemeriksaan multikolienaritas pada penelitian ini dilakukan dengan melihat nilai *Variance Inflation Factors* (VIF). Berdasarkan hasil pemeriksaan nonmultikolienaritas, tidak terdapat nilai VIF pada variabel independen yang lebih dari 10. Hasil pengujian menunjukkan bahwa model tidak mengandung multikolienaritas.

Pada penelitian ini model yang digunakan menghasilkan nilai *Adjusted* R^2 sebesar 0,5261. Artinya 52,61% GCI di ASEAN dapat dijelaskan oleh variabel pertumbuhan ekonomi, pengguna *mobile broadband,* pengguna *mobile cellular,* ekspor teknologi, RLS, dan indeks persepsi korupsi. Sedangkan 47,39% sisanya dijelaskan oleh variabel lain yang tidak tercakup dalam penelitian. Berdasarkan hasil uji simultan yang telah dilakukan diperoleh nilai *F-statistic* sebesar 11,939 dengan *p-value* sebesar 0,000. Hasil tersebut memberikan keputusan tolak H_0. Oleh karena itu, dapat disimpulkan bahwa minimal terdapat satu variabel yang signifikan memengaruhi GCI di ASEAN. Selanjutnya, pengujian parsial dilakukan dengan uji statistik t. Berdasarkan pengujian yang telah dilakukan variabel pertumbuhan ekonomi, pengguna *mobile broadband,* dan RLS mengahasilkan nilai *p-value* kurang dari 0,05. Sedangkan variabel pengguna *mobile celluler,* ekspor teknologi, dan indeks persepsi korupsi menghasilkan nilai *p-value* lebih dari 0,05. Hasil tersebut dapat diartikan bahwa variabel pertumbuhan ekonomi, pengguna *mobile broadband,* dan RLS berpengaruh secara signifikan terhadap GCI di ASEAN, sedangkan variabel pengguna *mobile celluler,* ekspor teknologi, dan indeks persepsi korupsi tidak berpengaruh secara signifikan terhadap GCI di ASEAN.

TABEL 2. Hasil estimasi Random Effect Model

Variabel	Koefisien	*t-statistic*	*P-value*
(1)	(2)	(3)	(4)
C	-109,277	-2,574964	0,0129*
PE	-1,050	-2,119774	0,0387*
MB	0,275	2,559579	0,0134*

MC	-0,100	-0,835903	0,4070
ET	0,257	0,882752	0,3814
LNRLS	86,530	2,961275	0,0046*
CPI	-0,620	-1,682226	0,0984

Sumber: data diolah menggunakan E-views 12
Keterangan: *) Signifikan pada $\propto$= 5%

Berdasakan hasil estimasi REM tersebut dapat dibentuk suatu persamaan sebagai berikut:

$$\widehat{GCI_{it}} = -109{,}277 - 1{,}050PE_{it}{}^{*} + 0{,}275\,MB_{it}{}^{*} - 0{,}100MC_{it} + 0{,}257ET_{it} + 86{,}530LnRLS^{*} - 0{,}620CPI_{it} \quad (1)$$

Berdasarkan hasil pengujian yang ditunjukkan oleh tabel 1, Nilai konstanta tidak berarti karena variabel independen tidak memiliki kemungkinan untuk bernilai nol. Pertumbuhan ekonomi menunjukkan hasil yang signifikan terhadap *Global Cybersecurity Index* di ASEAN. Setiap kenaikan 1% pertumbuhan ekonomi dapat menurunkan GCI sebesar 1,050 dengan asumsi variabel bebas lainnya konstan. Hal tersebut sejalan dengan penelitian Srivastava et al. (2020) yang menyatakan bahwa negara-negara yang memiliki standar ekonomi yang lebih baik mungkin memiliki teknologi yang lebih baik, komputer siap pakai, dan internet lebih canggih. Hal tersebut memberikan fasilitas untuk melakukan kejahatan lebih mudah dan membuat keamanan lebih rentan. Temuan pada penelitian ini juga sejalan dengan penelitian Solano et al. (2017) bahwa PDB dapat menambah jumlah *cybercrime* atau serangan di dunia siber sehingga keamanannya menurun.

Sementara itu, pengguna m*obile broadband* menunjukkan hasil yang signifikan terhadap GCI di ASEAN. Setiap kenaikan 1% pengguna *mobile broadband* dapat menaikkan GCI sebesar 0,275 poin dengan asumsi variabel bebas lainnya konstan. Hal tersebut sejalan dengan penelitian Makridis & Smeets (2019) yang menyebutkan bahwa negara yang memiliki kebergantungan internet tinggi, juga memiliki kesiapan siber yang lebih baik. Apabila suatu negara memiliki kesiapan siber yang baik, maka akan meningkatkan keamanan siber di negara tersebut.

RLS menunjukkan hasil yang signifikan terhadap GCI di ASEAN. Setiap kenaikan 1% RLS di ASEAN dapat menaikkan GCI sebesar 0,865 poin dengan asumsi variabel bebas lainnya konstan. Menurut Simon et al. (2018) pendidikan adalah proses membantu peserta didik untuk menyesuaikan diri dengan dunia yang selalu berubah. Salah satunya teknologi baru yang juga menciptakan peluang kriminal baru sebagai jenis kejahatan baru. Oleh karenanya, pendidikan dapat memberikan wawasan seseorang dalam melakukan pencegahan terhadap jenis kejahatan baru, yaitu *cybercrime*. Dengan demikian, semakin tinggi pendidikan, kecakapan dalam menjaga keamanan siber akan semakin baik.

Indeks persepsi korupsi menunjukkan hasil yang tidak signifikan berpengaruh terhadap GCI di ASEAN. Hal tersebut sejalan dengan temuan Srivastava et al. (2020) yang menyatakan bahwa CPI tidak memengaruhi *cybercrime*. Begitu juga dengan pengguna *mobile cellular,* tidak berpengaruh signifikan terhadap GCI. Abidin (2015) menyatakan bahwa *cybercrime* sering terjadi pada akun dan jejaring sosial internet. Saat ini ASEAN merupakan wilayah dengan era digitalisasi, sehingga internet tidak hanya di akses melalui *mobile cellular*. Khususnya pada sektor pemerintahan dan lembaga resmi, kegiatan penyimpanan data dan pengelolaan akun media sosial dan lainnya tidak selalu pada *mobile cellular*. Oleh karenanya, sarana utama pelaku *cybercrime* adalah internet, bukan *mobile cellular*. Berdasarkan hasil pengujian yang ditunjukkan oleh tabel 1, ekspor teknologi menunjukkan hasil yang tidak signifikan berpengaruh terhadap GCI di ASEAN. Ekspor teknologi di ASEAN melalui beberapa tahapan dan prosedur yang panjang. Sedangkan menurut Narwal et al. (2019) sebagian besar penyerang siber menggunakan perangkat serangan yang mudah dan tak terbatas untuk mendapatkan korban dengan tujuan memperoleh keuntungan finansial. Oleh karena itu, pelaku *cybercrime* tidak menjadikan ekspor teknologi sebagai sarana penyerangan. Tanpa melalui aktivitas lintas negara seperti ekspor dan impor, *cybercrime* sudah mampu menembus batas internasional melalui ruang siber.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian diperoleh kesimpulan sebagai berikut:

1. Nilai GCI di ASEAN sebagian besar mengalami kenaikan. Namun, masih terdapat kesenjangan nilai GCI yang sangat jauh antar negara di ASEAN. Negara dengan GCI tertinggi atau memiliki keamanan siber yang baik yaitu Singapura dan Malaysia. Sedangkan negara dengan nilai GCI terbawah di ASEAN yaitu Laos, Myanmar, dan Kamboja.
2. Pertumbuhan ekonomi, pengguna mobile broadband, dan RLS berpengaruh secara signifikan terhadap GCI, sedangkan pengguna mobile cellular, ekspor teknologi, dan indeks persepsi korupsi tidak berpengaruh secara signifikan terhadap GCI di ASEAN.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang diberikan, antara lain :

1. Untuk pemerintah negara-negara di ASEAN diharapkan terus meningkatkan perhatian terhadap keamanan siber di masing-masing negaranya. Utamanya pada pengembangan kapabilitas penduduk terhadap dunia siber. Apabila pengetahuan penduduk dalam dunia siber baik, diharapkan mampu berkontribusi untuk menjaga keamanan siber. Selain itu, masing-masing negara perlu memperluas kerjasama internasional dan memperkuat hukum tentang keamanan siber, khususnya bagi negara yang masih rendah nilai GCI nya. Lebih lanjut perlu dilakukan peningkatan sinergi dan sosialisasi dari organisasi keamanan siber berkaitan dengan cara berada dalam dunia siber yang aman.
2. Pemerintah negara-negara di ASEAN juga diharapkan mampu mengalokasikan anggaran untuk pelaksanaan teknis keamanan siber. Selain itu, pemerintah sebaiknya menjaga stabilitas jumlah pengguna mobile broadband, dan meningkatkan rata-rata lama sekolah di masing-masing negara.
3. Untuk penelitian selanjutnya dapat dilakukan penelitian dengan jenis *cybercrime* yang lebih spesifik, seperti phising, ransomware, cyber fraud, dan lain-lain. Dengan begitu, pencegahan dan penganan cybercrime di ASEAN menjadi lebih terfokus dan efektif.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih pada Politeknik Statistika STIS atas dukungannya.

REFERENSI

Algar, C. (2018, June 12). *Viet Nam: New Cybersecurity law a devastating blow for freedom of expression*. Amnesty International. https://www.amnesty.org/en/latest/news/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/

Avirutha, A. (n.d.). ASEAN in Digital Economy: Opportunities and Challenges. In *Journal of ASEAN PLUS + Studies* (Vol. 2, Issue 1).

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars. *Social Indicators Research*, *159*(1), 125–143. https://doi.org/10.1007/s11205-021-02739-y

Charoen, D. (2018). Digital Thailand. *NIDA Case Research Journal*, *10*(2).

Chuchu, F. Awg., & Abd Gafur, Muhd. K. A. (2020). *Cyber Crime in Brunei Darussalam Viewed from Sociological Perspective*. 354–361. https://doi.org/10.5220/0008885103540361

Cyber Security Agency of Singapore. (2016). *Singapore's cybersecurity strategy.*

Cyber Security Agency of Singapore. (2021, October 5). *The Singapore Cybersecurity Strategy 2021*. CSA Singapore.

Danuri, M., Informatika, M., Teknologi, J., & Semarang, C. (n.d.). *PERKEMBANGAN DAN TRANSFORMASI TEKNOLOGI DIGITAL*.

Deora, R. S., & Chudasama, D. M. (2021). *Brief Study of Cybercrime on an Internet Information Systems Audits for eCommerce View project Grocery Deals View project*. https://doi.org/10.37591/JoCES

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Dwi Aprilia, N., Djoko Waluyo, S., Saragih, H. J., Pertahanan, E., Pertahanan, M., & Pertahanan, U. (n.d.). *PERKEMBANGAN EKONOMI DIGITAL INDONESIA THE DEVELOPMENT OF INDONESIA'S DIGITAL ECONOMY*.

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). CYBERSECURITY INDICES AND CYBERCRIME ANNUAL LOSS AND ECONOMIC IMPACTS. *Journal of Business and Behavioral Sciences*, *32*(1). http://www.asbbs.org

Fardani, N. E. (2015). *Analisis Faktor-Faktor yang Mempengaruhi Loyalitas Pelanggan Mobile Broadband Services Telkomsel di Kota Bandung Tahun 2014*.

Global Coalition to Protect Education from Attack. (2018, May 11). *Education Under Attack 2018 - The Philippines*. Global Coalition to Protect Education from Attack. https://www.refworld.org/docid/5be942ffa.html

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, *38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Gujarati, D., & Porter, D. (2009). Basic Econometric

Islami, M. J. (2017). TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX. *Jurnal Masyarakat Telematika Dan Informasi* , *8*, 137–144.

Kristiani Virgi Kusuma Putri Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime 543. (n.d.). https://jhlg.rewangrencang.com/

Kurniasih, E. P. (2020). *Prosiding Seminar Akademik Tahunan Ilmu Ekonomi dan Studi Pembangunan*.

Kusumastuti, A., & Nuryani, A. F. (2019). Digital Literacy Level in ASEAN (Comparative Study in ASEAN Countries). In G. T. I. Tawakkal, Wike, N. Harahab, A. Utaminingsih, & A. S. Leksono (Eds.), *IISS 2019: Proceedings of the 13th International Interdisciplinary Studies* (pp. 269–279).

Lin, C., & Geddie, J. (2021). *Singapore COVID-19 contact-tracing data accessible to police*. Reuters. https://www.reuters.com/business/healthcare-pharmaceuticals/singapore-covid-19-contact-tracing-data-accessible-police-2021-01-04/

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, *4*(1), 72–89. https://doi.org/10.1080/23738871.2019.1604781

Marmita, S. (2020). Struggle of ASEAN in cyber security. *Asia and Africa Today*, *8*, 52. https://doi.org/10.31857/s032150750010451-8

Maskun, M., Irwansyah, I., Yunus, A., Safira, A., & Lubis, S. N. (2021). Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with it. *Jambe Law Journal*, *4*(2), 131–150. https://doi.org/10.22437/jlj.4.2.131-150

Nguyen, M. (2018, June 12). *Vietnam lawmakers approve cyber law clamping down on tech firms, dissent*. Reuters. https://www.reuters.com/article/us-vietnam-socialmedia-idUSKBN1J80AE

Nugraha, R. (2021). *PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA* (Vol. 11, Issue 2).

Pradono, W. (2021). Analysis on Competition Type between Fixed and Mobile Broadband Service in Indonesia. *Buletin Pos Dan Telekomunikasi*, *19*(2), 97. https://doi.org/10.17933/bpostel.2021.190202

Reis, J., Amorim, M., Melão, N., Cohen, Y., & Rodrigues, M. (2020). *Digitalization: A Literature Review and Research Agenda* (pp. 443–456). https://doi.org/10.1007/978-3-030-43616-2_47

Simon,] A, Veliappan, A., Scholar,] M Ed, & Assistant,]. (2018). Impact of Cyber Crimes and Education. In *International Journal of Science, Engineering and Management (IJSEM)* (Vol. 3).

Siregar, G. T., & Sinaga, S. (2021). THE LAW GLOBALIZATION IN CYBERCRIME PREVENTION. *International Journal of Law Reconstruction*, *5*(2), 211. https://doi.org/10.26532/ijlr.v5i2.17514

Solano, P. C., José, A., & Peinado, R. (2017). *Socio-economic factors in Cybercrime: Statistical study of the relation between socio-economic factors and cybercrime*. http://data.uis.unesco.org

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, *23*(2), 112–137. https://doi.org/10.1080/1097198X.2020.1752084

Suyatmiko, W. H. (2021). Memaknai Turunnya Skor Indeks Persepsi Korupsi Indonesia Tahun 2020. *INTEGRITAS*, *7*(1), 161–178. https://doi.org/10.32697/integritas.v7i1.717

Sviatun, O. v., Goncharuk, O. v., Chernysh, R., Kuzmenko, O., & Kozych, I. v. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751–762. https://doi.org/10.37394/23207.2021.18.72

Tatarinovaa, L. F., Shakirov, K. N., & Tatarinov, D. V. (2016). *criminological-analysis-of-determinants-of-cybercrime-technologies*.

UN. (2021, May 28). *Strengthening digital capacities and skills to meet the demands of the digital world*.

UNODC. (2019, March). *Reporting cybercrime*. UNODC. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html

Viano, E. C. (2017). Cybercrime: Definition, Typology, and Criminalization. In *Cybercrime, Organized Crime, and Societal Responses* (pp. 3–22). Springer International Publishing. https://doi.org/10.1007/978-3-319-44501-4_1

Wibowo, E. W. (2018). *ANALISIS EKONOMI DIGITAL DAN KETERBUKAAN TERHADAP PERTUMBUHAN GDP NEGARA ASEAN* (Vol. 7, Issue 2).

Wicaksana, N. R. F. (2018). *Analisis Pengaruh Akses Teknologi Informasi dan Komunikasi Terhadap Pertumbuhan Ekonomi*.