Implikasi Cybercrime Pada Bisnis Digital di Indonesia

Aria Devananta
Universitas Brawijaya
ariadvnt@gmail.com

ABSTRAK

Kemajuan teknologi memberikan pengaruh negatif dan positif terhadap teknologi saat ini. Mulai dari berita yang mungkin bisa kita lihat di media sosial terdapat informasi yang berguna bagi kita untuk bisa memaksimalkan segala aktivitas yang ada saat ini. Seluruh aktivitas dapat berjalan dengan cepat dan praktis sehingga sangat membantu karena bantuan teknologi. Dampak positif perkembangan teknologi saat ini dapat mempermudah mencari informasi dan mempermudah pekerjaan tergantung bagaimana teknologi dapat menguntungkan sebuah bisnis. Dampak negatif dari perkembangan teknologi adalah munculnya *cybercrime* di dunia maya. Tujuan penelitian ini berusaha menjelaskan kembali secara deskriptif mengenai fenomena *cybercrime* yang terjadi pada bisnis digital di Indonesia. Metode penelitian yang digunakan pada penelitian ini adalah deskriptif kuantitatif yang mencoba mengumpulkan informasi yang dapat diukur untuk dianalisis. Hasil penelitian ini menjelaskan bahwa ancaman baru terus mengalami peningkatan pada bisnis digital yang semakin berkembang di Indonesia. Penegakan hukum terhadap *cybercrime* yang masih sangat minim membuat *cybercrime* masih bebas di Indonesia, hal ini dikarenakan peraturan perundang-undangan yang ada di Indonesia harus terus diperbaharui seperti negara maju lainnya sebagai langkah preventif dari serangan *cybercrime* yang dapat mengancam bisnis digital saat ini.
Kata Kunci: *Cybercrime*, bisnis digital, Indonesia.

ABSTRACT

Technological advances have a negative and positive influence on today's technology. Starting from the news that we might be able to see on social media, there is useful information for us to be able to maximize all the activities that are currently available. All activities can run quickly and practically so it is very helpful because of the help of technology. The positive impact of current technological developments can make it easier to find information and make work easier depending on how technology can benefit a business. The negative impact of technological developments is the emergence of cybercrime in cyberspace. The purpose of this study is to describe descriptively about the cybercrime phenomenon that occurs in digital businesses in Indonesia. The research method used in this research is descriptive quantitative which tries to collect measurable information for analysis. The results of this study explain that new threats continue to increase in the growing digital business in Indonesia. Law enforcement against cybercrime which is still very minimal makes cybercrime still free in Indonesia, this is because the existing laws and regulations in Indonesia must continue to be updated like other developed countries as a preventive measure from cybercrime attacks that can threaten today's digital business.
Keywords: *Cybercrime, Digital Business, Indonesia*

PENDAHULUAN

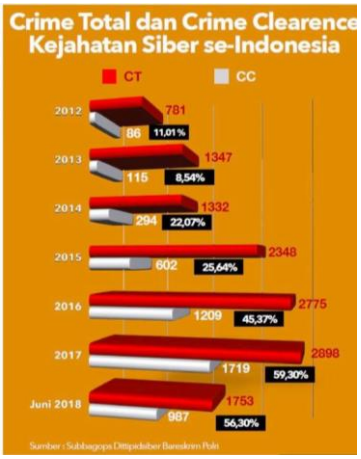
Perkembangan teknologi baru menciptakan peluang kriminal baru dalam penggunaan komputer yang selalu mengalami kemajuan, kejahatan dapat mengikuti kemajuan teknologi sebagai langkah perluasan tindakan pelaku kejahatan. Tanpa internet, kriminalitas seperti perampokan dan pencurian data seseorang telah berlangsung lama. Semua ini terjadi sebelum istilah "*cyber*" digunakan secara luas. *Cybercrime* merupakan kejahatan yang berada pada dunia maya, kemajuan pada teknologi informasi seperti internet ini dapat digunakan sebagai tindakan ilegal sebelumnya serta beberapa perilaku ilegal baru (Conteh, 2021). Mayoritas *cybercrime* menargetkan informasi pribadi, perusahaan, atau pemerintah, meskipun serangan tidak menargetkan tubuh fisik seseorang, mereka menargetkan identitas virtual seseorang atau perusahaan, yang merupakan serangkaian data digital yang menggambarkan seseorang individu dan institusi di Internet. Dengan kata lain, di era digital, identitas virtual kita adalah bagian penting dari kehidupan sehari-hari, kita adalah kumpulan angka dan pengenal yang disimpan di banyak

database komputer pemerintah dan perusahaan. *Cybercrime* menekankan pentingnya jaringan komputer dalam kehidupan kita, serta fakta bahwa data kita tidak pernah aman di jaringan internet (Palmieri, Shortland, & McGarry, 2021).

Fitur utama pada internet adalah lintas batas negara, tindakan kejahatan dalam internet dapat terjadi di negara-negara yang dipisahkan oleh jarak yang sangat jauh. Hal ini menimbulkan kesulitan yang signifikan bagi penegakan hukum karena kejahatan lokal atau bahkan nasional sebelumnya memerlukan kerjasama internasional. Misalnya, apakah seseorang yang mengakses pornografi anak di komputer di negara yang tidak melarang pornografi anak melakukan kejahatan di negara yang tindakan tersebut dilarang? Ketika muncul *cybercrime*, di mana itu terjadi? *Cyberspace* pada dasarnya adalah bentuk yang lebih berkembang dari ruang di mana panggilan telepon terjadi, di suatu tempat antara dua orang yang sedang berbicara. Internet, sebagai jaringan global, menyediakan beberapa tempat persembunyian bagi para penjahat baik di dunia nyata maupun di dalam jaringan itu sendiri. Penjahat dunia maya, seperti orang yang berjalan di tanah, meninggalkan tanda tentang identitas dan keberadaan mereka yang dapat diikuti oleh pelacak. Namun, seperti halnya orang yang berjalan di tanah meninggalkan jejak yang dapat diikuti oleh pelacak, peretas meninggalkan jejak identitas dan keberadaan mereka, terlepas dari upaya terbaik mereka untuk menyembunyikan jejak mereka (Lusthaus & Varese, 2021).

Cybercrime hampir terjadi di seluruh spektrum kegiatan. Di satu sisi adalah kejahatan yang melibatkan pelanggaran mendasar privasi pribadi atau perusahaan, seperti serangan terhadap integritas informasi yang disimpan dalam penyimpanan digital dan penggunaan informasi digital yang diperoleh secara ilegal untuk memeras perusahaan atau individu. Juga di ujung spektrum ini adalah meningkatnya kejahatan pencurian identitas. Di tengah-tengah spektrum terdapat kejahatan berbasis transaksi seperti penipuan, perdagangan pornografi anak, pembajakan digital, pencucian uang, dan pemalsuan. Ini adalah kejahatan khusus dengan korban tertentu, tetapi penjahat bersembunyi dalam anonimitas relatif yang disediakan oleh Internet. Bagian lain dari jenis kejahatan ini melibatkan individu dalam perusahaan atau birokrasi pemerintah dengan sengaja mengubah data untuk tujuan keuntungan atau politik. Di ujung lain spektrum adalah kejahatan yang melibatkan upaya untuk mengganggu cara kerja Internet yang sebenarnya. Ini berkisar dari spam, peretasan, dan serangan penolakan layanan terhadap situs tertentu hingga tindakan terorisme siber yaitu, penggunaan Internet untuk menyebabkan gangguan publik dan bahkan kematian. *Cyberterrorism* berfokus pada penggunaan Internet oleh aktor non-negara untuk mempengaruhi infrastruktur ekonomi dan teknologi suatu negara. Sejak serangan 11 September 2001, kesadaran publik akan ancaman terorisme siber telah tumbuh secara dramatis (Marsili, 2019). Perkembangan digital saat ini semakin cepat, seperti akses internet yang lebih mudah dan murah (Tiago & Veríssimo, 2014). Internet yang berkembang telah menyebabkan perubahan besar dalam cara pemasar bekerja dan menggunakan strategi pemasaran. Penelitian sebelumnya menunjukkan bahwa pemasaran tradisional yang dilakukan perusahaan untuk meningkatkan penjualan, seperti televisi, majalah, dan radio, dianggap tidak stabil (Opreana & Vinerean, 2015; Tiago & Veríssimo, 2014). Pemasaran tradisional dianggap usang karena internet telah mengubah pasar dan kehilangan efektivitasnya.

Indonesia merupakan penyumbang serangan *cybercrime* terbesar kedua setelah Tiongkok, menurut data yang dirilis oleh Kementerian Komunikasi dan Informatika pada tahun 2013. Dalam tiga tahun tersebut, 36,6 juta kejadian *cybercrime* terjadi di Indonesia. Total kejahatan dan pembersihan kejahatan (jumlah kasus yang dilaporkan dan jumlah kasus yang diselesaikan dalam jangka waktu tertentu). Jumlah kejahatan yang “dihapus” (tuduhan dijatuhkan) dibagi dengan jumlah total kejahatan yang dilaporkan untuk mencapai peringkat ini. Berbagai pihak menggunakan *Crime Total* dan *Clearance Rate* sebagai indikator berapa banyak kejahatan yang telah diselesaikan polisi. *Clearance Rate* dapat membuat evaluasi kinerja polisi dan membandingkan kinerja. Ini karena fakta bahwa departemen kepolisian yang berbeda dapat menghitung tingkat penyelesaian dengan cara yang berbeda. Setiap departemen kepolisian, misalnya, mungkin menggunakan prosedur yang berbeda untuk merekam ketika "kejahatan" telah terjadi dan kriteria yang berbeda untuk menilai kapan suatu kejahatan telah "dibersihkan." Karena prosedur penghitungannya berbeda, satu lembaga kepolisian mungkin tampak memiliki tingkat penyelesaian yang jauh lebih tinggi. Menurut Teori Sistem Konflik, tingkat kelengkapan menyebabkan polisi fokus pada penyelesaian kejahatan daripada benar-benar menyelesaikan kejahatan (menghasilkan skor tingkat penyelesaian yang tinggi). Berfokus pada tingkat yang lebih berisiko dapat mengarah pada upaya untuk menghubungkan kejahatan dengan pelanggar, yang mungkin tidak menghasilkan retribusi, kompensasi, rehabilitasi, atau pencegahan.



Gambar 1. Data Serangan *Crime Total* dan *Crime Clearance* Kejahatan Siber di Indonesia Tahun 2012 sampai dengan 2018
Sumber : Subbagops Ditipisiber Bareskrim Polri

Menurut temuan studi Frost and Sullivan yang dilakukan oleh Microsoft, potensi kerugian ekonomi di Indonesia yang disebabkan oleh insiden keamanan siber bisa mencapai USD 34,2 miliar, atau Rp 483 triliun (kurs Rp 14.120 per USD). Jumlah ini setara dengan 3,7 persen dari total PDB Indonesia sebesar USD 932 miliar. Selain kerugian finansial, peristiwa keamanan siber membatasi kemampuan banyak perusahaan di Indonesia untuk memanfaatkan prospek ekonomi digital saat ini. Tiga perlima responden (61%) mengindikasikan organisasi mereka telah menunda upaya transformasi digital karena kekhawatiran tentang bahaya dunia maya. Dengan diumumkannya rencana kerja Making Indonesia 4.0 oleh Presiden Joko Widodo dan Kementerian Perindustrian Republik Indonesia, transformasi digital menjadi semakin penting bagi dunia usaha. Hal ini dapat menjadi penghalang bagi organisasi Indonesia yang mencoba untuk menyelaraskan taktik berdasarkan rencana kerja (Anderson et al., 2013).

Studi yang berjudul *'Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World'* berupaya memberikan perspektif mendalam tentang dampak ekonomi dari serangan siber di Asia dan Indonesia bagi para pembuat kebijakan bisnis dan TI, serta menyoroti kesenjangan dalam kebijakan keamanan siber. Selain kerugian finansial yang jelas terkait dengan serangan keamanan siber, seperti hilangnya produktivitas, denda, dan biaya perbaikan, ada juga biaya tidak langsung, seperti hilangnya kemungkinan bisnis untuk menciptakan hubungan pelanggan yang kuat karena kerusakan reputasi. Belum lagi dampak serangan siber pada ekosistem dan ekonomi yang lebih besar, seperti pengurangan belanja pelanggan dan perusahaan. Menurut laporan tersebut, sebuah organisasi berskala besar di Indonesia kemungkinan akan kehilangan USD 16,3 juta, yang merupakan 200 kali kerugian ekonomi rata-rata perusahaan menengah. Belum lagi dampak serangan siber pada ekosistem dan ekonomi yang lebih besar, seperti pengurangan belanja pelanggan dan perusahaan. Menurut laporan tersebut, sebuah organisasi berskala besar di Indonesia kemungkinan akan kehilangan USD 16,3 juta, yang merupakan 200 kali kerugian ekonomi rata-rata perusahaan menengah (Hermawan, 2015). Pelaku kejahatan ini biasanya adalah mereka yang memiliki pengetahuan yang lebih baik tentang teknologi dan memanfaatkan pengetahuan itu untuk mendapatkan akses tidak sah ke jaringan komputer orang lain. Akibatnya, tren penjahat dunia maya menjadi jelas: mereka yang mengerti dan terampil di dunia maya. Peningkatan kejahatan dunia maya baru-baru ini memerlukan pendekatan penegakan hukum yang terkoordinasi yang dipimpin oleh polisi. Topik "polisi siber" mengemuka dalam perbincangan, begitu pula kekhawatiran banyak pihak yang tersinggung dengan ulah para hacker dan cracker di dunia maya. Hacker dan cracker telah mencuri data perusahaan penting dalam sejumlah situasi di sektor korporasi. Sementara itu, industri perbankan prihatin karena peretas dan cracker yang melakukan kejahatan dunia maya sering membahayakan keamanan jaringan. Bahkan, peretas kerap mengirimkan virus untuk merusak jaringan milik pemerintah, sehingga kedaulatan negara di dunia maya menjadi sangat berbahaya.

Di Indonesia, memang sudah ada Direktorat Tindak Pidana Siber di Bareskrim Polri yang menangani berbagai tindak pidana dunia maya. Namun demikian, kualifikasi maupun kompetensinya perlu ditingkatkan lagi sehingga mampu memberantas berbagai tindak kejahatan dunia maya yang marak belakangan ini. Perlu kiranya ke depan, Polri membentuk detasemen khusus dunia maya

dimana terdapat unit- unit khusus di setiap Polda dan Polres yang menangani tentang *cybercrime* sehingga akan lahir *cyber police* di lingkungan Polri untuk menegakan hukum terhadap setiap laporan masyarakat yang dirugikan dan menjadi korban dari aksi *cybercrime*. Selain itu, *munculnya cyber space* dan *cyber police* juga telah mendorong setiap negara di dunia, termasuk Indonesia untuk membentuk *cyber law* sehingga dapat dijadikan sebagai panduan dan payung hukum dalam menangani berbagai cybercrime sehingga *cyber security* Indonesia menjadi lebih aman dan nyaman. Di Indonesia sekarang ini, baru ada UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), sehingga belum ada lagi aturan hukum atau *cyber law* lainnya sebagai dasar dalam menegakan hukum terhadap kasus-kasus dan kejahatan *cybercrime*.

Pemerintah harus lebih peka dan waspada terhadap serangan *cybercrime*, tren menunjukkan pertumbuhan besar dalam serangan perusakan web, yang dapat menguasai situs web pemerintah dan menggunakannya untuk tujuan yang tidak bertanggung jawab, atau bahkan mengganti tampilan web dengan tampilan yang berbeda. Di Indonesia perlu adanya strategi pencegahan kejahatan berbasis internet yang dapat diterima oleh semua lapisan masyarakat dan pengguna internet serta berbasis budaya lokal.

METODE

Penelitian ini menggunakan teknik deskriptif kuantitatif, di mana penulis mengumpulkan data historis dan memperhatikan fitur-fitur tertentu dari subjek yang diselidiki untuk mendapatkan data yang akan membantu dalam pengembangan laporan penelitian (Saunders et al., 2009). Data tersebut kemudian diolah dan diteliti lebih lanjut berdasarkan teori yang telah dipelajari untuk memperoleh pemahaman yang lebih baik tentang objek dan membentuk kesimpulan tentang topik yang diteliti (Sekaran & Bougie, 2016). Perusahaan digital dan badan pemerintah terkait yang secara langsung menangani kejahatan dunia maya yang terjadi di Indonesia melalui internet menjadi subjek penelitian. Penulis menggunakan metode deskriptif dan asosiatif dalam penyusunan jurnal ini, karena faktor-faktor yang akan diteliti terkait dengan hal tersebut, prosedur kasus berusaha memberikan penjelasan yang sistematis, faktual, dan benar mengenai fakta dan keterkaitan antar variabel yang akan dianalisis Dengan maraknya *cybercrime* dalam ekonomi digital, khususnya di ekonomi digital.

Peneliti dapat mengumpulkan informasi dari berbagai sumber tertulis atau makalah yang ada di rumah atau tempat usaha responden. Baxter dan Jack (2008) Tujuan dari dokumentasi penjelasan adalah untuk mendapatkan data langsung dari lokasi penelitian, seperti buku-buku yang relevan. Ada tiga jenis dokumen dalam penelitian pendidikan: makalah primer, sekunder, dan tersier, masing-masing dengan tingkat legitimasi yang berbeda. Lind et al. (2018) menunjukkan bahwa menggunakan pendekatan dokumentasi adalah cara lain untuk mendapatkan data dari responden. Metode pemilihan informan adalah jenis *purposive sampling*. Orang-orang dipilih untuk prosedur ini berdasarkan seperangkat kriteria yang dibuat oleh peneliti dan tergantung pada tujuan penelitian. Orang-orang yang tidak memenuhi persyaratan ini tidak diambil sampelnya sementara itu. Menurut Moleong (2021), Subyek yang telah lama terintegrasi kuat dengan suatu kegiatan atau bidang kegiatan yang menjadi topik atau perhatian penelitian, dan hal ini sering ditentukan oleh kemampuannya untuk memberikan informasi dengan hati tentang sesuatu yang ditanyakan, dianggap sebagai informan. Subjek tetap sepenuhnya terlibat dan terlibat dalam lingkungan dan kegiatan yang sedang dipelajari. Subyek diberikan waktu dan kesempatan yang cukup untuk memberikan informasi. Subyek yang menjadi sukarelawan informasi biasanya tidak diproses atau dikemas sebelumnya, dan mereka masih relatif polos ketika melakukannya (Moleong, 2021).

Analisis data adalah suatu metode untuk mengubah data menjadi informasi sehingga sifat-sifat data tersebut dapat dengan mudah dipahami dan diterapkan untuk memecahkan masalah yang berkaitan dengan penelitian. Selanjutnya, analisis data dapat diartikan sebagai tindakan mencari dan menyusun transkrip wawancara, catatan lapangan, dan bahan-bahan lain yang telah diperoleh secara sistematis atau Peneliti membuat laporan ini setelah mengumpulkan data dari lapangan. Kegiatan analisis data ini meliputi penelaahan data, pengorganisasian, dan pemisahannya menjadi unit-unit sehingga dapat dikendalikan dan diketahui makna sebenarnya dari data tersebut sesuai dengan rumusan masalah yang telah ditetapkan. Analisis data dalam penelitian ini dilakukan sejak sebelum memasuki lapangan, selama di lapangan, dan setelah dilapangan selesai Penelitian ini lebih merupakan gambaran hasil wawancara dan studi dokumentasi daripada studi ilmiah. Data tersebut akan diteliti secara statistik dengan menggunakan indikator-indikator tertentu berdasarkan

pertanyaan wawancara terstruktur dan dimensi topik penelitian, kemudian dirangkum dalam bentuk deskriptif (Moleong, 2021).

Analisis data diakhiri dengan verifikasi dan konfirmasi kesimpulan. Kesimpulan dicapai melalui proses interpretatif, yang memerlukan penentuan signifikansi bukti yang diberikan. Operasi analisis data yang ada berkisar dari menampilkan data hingga mengembangkan kesimpulan. Dengan cara ini, analisis data kualitatif adalah proses yang tidak pernah berakhir, berulang, dan berkelanjutan. Sebagai rangkaian tindakan analitis yang terkait, masalah reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi menghasilkan gambaran keberhasilan. Selanjutnya data yang telah dipelajari, dijelaskan, dan diinterpretasikan dalam bentuk kata-kata untuk menggambarkan fakta di lapangan, maknanya, atau untuk menjawab pertanyaan penelitian yang kemudian digali dari esensinya. Berdasarkan keterangan di atas, maka setiap tahapan proses dilakukan untuk memastikan keabsahan data dengan menelaah semua data yang ada dari berbagai sumber seperti dokumen lapangan dan pribadi, dokumen dinas, gambar, dan foto antara lain menggunakan metode wawancara yang didukung dengan studi dokumentasi (Baxter & Jack, 2008).

HASIL

Menurut penelitian sebelumnya, kejahatan dunia maya menjadi perhatian dunia. Beberapa negara industri dengan korporasi global besar, khususnya di sektor bisnis digital, menjadi sasaran *cybercrime global*. Karena ancaman kejahatan dunia maya lebih besar di negara-negara industri daripada di negara-negara miskin, negara-negara ini memberlakukan banyak undang-undang sebagai tindakan pencegahan. Penyelesaian kasus dilakukan dengan sangat serius dan penuh perhatian, terutama dalam ekonomi digital, karena kejahatan dunia maya mengakibatkan kerugian yang signifikan bagi bisnis. *Cybercrime* menghasilkan banyak uang di dunia online, oleh karena itu ada banyak bahaya bagi perusahaan digital yang berisiko tinggi, mulai dari data pelanggan hingga data akun dan pembayaran dari pelanggan.

Gambar 2. Cybercrime Annual Revenues
Sumber: *https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/*

Pendapatan Tahunan dari Kejahatan Dunia Maya Jika kita menganggap bahwa lebih dari setengah serangan kejahatan dunia maya terbesar terjadi di pasar *online*, total nilai tahunannya adalah USD 1,5 triliun. Hal ini menunjukkan bahwa perusahaan digital, terutama yang memiliki platform, berisiko tinggi menjadi korban kejahatan dunia maya.

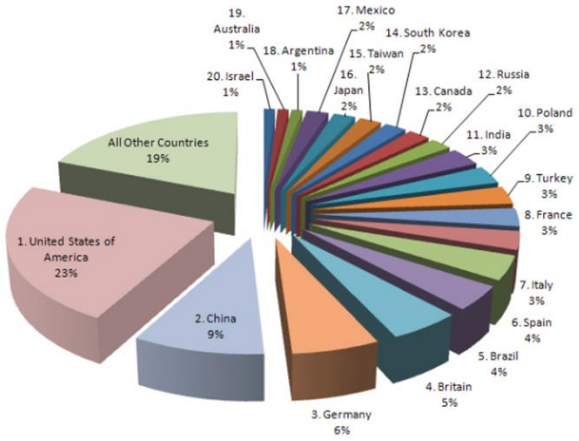
Tabel 1. Cybercrime Annual Revenues in Online Markets

Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware/CaaS	$1.6 Billion
Ransomware	$1 Billion
Total Cybercrime Revenues	$1.5 Trillion

FACT: Over 50% of cybercrime revenues are generated in online markets.

Sumber: *https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually*

Pada tahun 2018, Amerika Serikat dan China termasuk di antara negara-negara yang paling ditargetkan di dunia, diikuti oleh negara-negara maju lainnya. Karena industri bisnis digital Indonesia meningkat pesat setiap tahun, besar kemungkinan Indonesia akan menjadi sasaran serangan di masa depan. Perluasan pasar online Indonesia telah disertai dengan peningkatan risiko serangan siber, yang telah menjadi ancaman bagi banyak bisnis digital di negara ini, khususnya e-commerce.



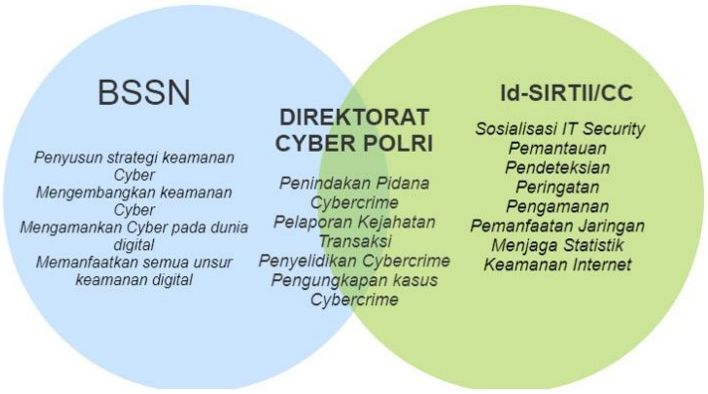
Gambar 3. *Cybercrime Top 20 Countries*
Sumber: *https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/*

BSSN menyusun Strategi Keamanan Siber Indonesia sebagai acuan tunggal bagi seluruh pelaku keamanan siber nasional dalam merancang dan melaksanakan kebijakan keamanan siber di instansi masing-masing, dan kemampuan beradaptasi. Pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya. Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. Tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber, dan keamanan siber dalam ekonomi digital merupakan tujuan strategis Strategi Keamanan Siber Indonesia. Dalam berbagai konferensi keamanan siber internasional, Strategi Keamanan Informasi Indonesia diharapkan dapat menjadi salah satu pilar kepercayaan dunia terhadap Indonesia. Strategi Keamanan Siber Indonesia merupakan komitmen pemerintah Indonesia untuk memajukan perdamaian dunia.

Gagasan untuk mendirikan Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center)* telah mulai disampaikan oleh beberapa kalangan khususnya praktisi, industri, akademisi, komunitas teknologi informasi dan Pemerintah sejak tahun 2005. Id-SIRTII/CC mempunyai tanggung jawab utama untuk melakukan sosialisasi IT Security (keamanan sistem informasi) dengan pihak terkait, melakukan pemantauan dini, deteksi dini, dan peringatan dini terhadap ancaman jaringan telekomunikasi dari dalam dan luar negeri, khususnya dalam upaya pengamanan pemanfaatan jaringan, pembuatan/ menjalankan/mengembangkan file log database dan statistik keamanan Internet, dan membuat/menjalankan/mengembangkan file log database dan statistik keamanan Internet di Indonesia. Kerentanan keamanan sistem informasi dapat mengakibatkan ancaman, gangguan, dan serangan. Kemungkinan besar operasi ini akan mengakibatkan kerugian finansial dan penghentian layanan bagi pengguna. Di Indonesia, misalnya, hilangnya sumber daya internet semata-mata karena menumpuknya paket-paket informasi sampah akibat serangan pihak-pihak yang tidak bertanggung jawab. Id-SIRTII/CC memiliki fungsi pendukung dalam penegakan hukum, terutama dalam hal tindak pidana yang melibatkan teknologi informasi. Terutama dalam hal menyajikan bukti teknologi, Id-SIRTII/CC memiliki sumber daya, pengalaman, dan prosedur untuk melakukan analisis sehingga bukti material dapat digunakan di pengadilan. Dalam suatu penyidikan, Id-SIRTII/CC memiliki peran kunci dalam menyediakan data statistik lalu lintas internet Indonesia dan pola serangan (insiden).

Penanganan *cybercrime* pada Mabes Polri berada di Direktorat Tindak Pidana Siber Bareskrim Polri yang menangani tindak pidana antara lain tindak pidana yang terkait dengan cybercrime, tindak pidana informasi dan transaksi elektronik. Subdit Siber Direktorat Reserse Kriminal Khusus Polda

Metro Jaya, tugasnya adalah melakukan penyelidikan dan penyidikan tindak pidana khusus, terutama kegiatan penyidikan yang berhubungan dengan teknologi informasi, telekomunikasi, serta transaksi elektronik. Dengan pengungkapan kasus-kasus *cybercrime* yang terus meningkat dari waktu ke waktu, Subdit Siber Polda Metro Jaya nampak terus menyempurnakan sistem pengungkapan kejahatan dunia maya dan komputer. Jika kita merujuk pada penjelasan di atas maka penulis dapat membuat mapping pada lembaga-lembaga pemerintah terkait adalah sebagai berikut :



Gambar 4. Tugas BSSN, Direktorat TP SIBER Polri dan ID- SIRTII
Sumber: Penulis (2021)

Pemerintah berupaya untuk memaksimalkan keamanan di dunia digital, khususnya yang berkaitan dengan bisnis, maka dari itu dibentuklah organisasi-organisasi ini untuk melindungi perusahaan-perusahaan digital di Indonesia dari serangan *cybercrime*. Kejahatan dunia maya dapat dilawan oleh organisasi dan pengguna internet yang bekerja sama. Pengguna internet juga harus berhati-hati agar tidak menjadi korban penipuan *cyber* jenis ini. Untuk memerangi jenis kejahatan ini, pengguna, pemerintah, dan organisasi yang berpartisipasi di dunia digital harus bekerja sama. Dalam memerangi kejahatan dunia maya, pemerintah harus memimpin. Hukum dan peraturan yang kuat dapat membantu mengurangi kejahatan dunia maya.

KESIMPULAN

Berdasarkan temuan penelitian dan pembahasan temuan, dapat disimpulkan bahwa dunia bisnis saat ini menghadapi tantangan baru, dan kita harus mewaspadai serangan yang sedang naik daun dan dapat mengakibatkan kerugian yang cukup besar. Maraknya bisnis digital di Indonesia, khususnya E-Commerce, sejalan dengan bahaya di dunia digital yang dapat membahayakan bisnis digital di tanah air. Setiap tahun, kejahatan menghasilkan kerugian total USD 1,5 triliun. Pemerintah serius untuk mengembangkan di Indonesia untuk itu pemerintah menyiapkan segala perangkat yang diperlukan seperti halnya Undang Undang ITE, peraturan yang diperlukan, dan lembaga- lembaga yang terkait. Kemudian terkait bisnis digital harus mengetahui 4 Undang-Undang, pertama, Peraturan Pemerintah no 82 tahun 2012 tentang Penyelenggaraan Sistem dan Teransaksi Elektronik. Kedua, Undang-undang no 19 tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Ketiga, PermenKominfo no 10 tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik Instansi Penyelenggara Negara. Keempat, PermenKominfo no 7 tahun 2018, Melakukan pemetaan manajemen resiko dapat memakai indeks BSSN, Penerapan Standar, ISO 270001, IDSS, dan OSO. Karena perundang-undangan dan undang-undang yang ada di Indonesia, seperti yang ada di negara industri lainnya, harus terus diperbarui sebagai langkah preventif terhadap serangan cybercrime yang dapat membahayakan perusahaan digital saat ini, *cybercrime* tetap bebas di Indonesia.

SARAN

Pemerintah harus membuat aturan yang jelas mengenai *cybercrime* dan tindakan kejahatan digital lainnya secara detail di Indonesia, sehingga pelaku kejahatan digital tidak dapat leluasa melakukan kejahatan di dunia digital terutama pada bisnis *E-Commerce*. Kepolisian harus lebih aktif dalam menindak dan merespon laporan dari masyarakat terkait tindakan kejahatan *cybercrime* di Indonesia, langkah hukum yang jelas dan respon yang cepat diharapkan akan mengurangi tindakan *cybercrime* di Indonesia kedepannya. Peneliti selanjutnya diharapkan dapat menggunakan metode yang lebih aplikatif untuk mengukur *cybercrime* di Indonesia, karena penelitian mengenai

cybercrime di Indonesia masih sangat minim, dan kebutuhan akan kebijakan dan pembaruan regulasi dalam hal *cybercrime* sangat diperlukan untuk negara kita agar aturan terkait hal ini terus berkembang.

Daftar Pustaka

Buku dan Jurnal

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer.

APJII. (2017). *Hasil Survey Penetrasi dan Perilaku Pengguna Internet Indonesia 2017* (APJII).

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544–559.

Conteh, N. Y. (2021). The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention* (pp. 144–149). IGI Global.

Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, *6*(1), 43–50.

Lind, D. A., Marchal, W. G., & Wathen, S. A. (2018). *Statistical Techniques in Business & Economics* (17th ed., p. 897). McGraw Hill Education.

Lusthaus, J., & Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 4–14.

Marsili, M. (2019). The war on cyberterrorism. *Democracy and Security*, *15*(2), 172–199.

Moleong, L. J. (2021). *Metodologi penelitian kualitatif*. PT Remaja Rosdakarya.

Opreana, A., & Vinerean, S. (2015). A new development in online marketing: Introducing digital inbound marketing. *Expert Journal of Marketing*, *3*(1).

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, *120*, 106745.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). Prentice Hall.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.

Tiago, M. T. P. M. B., & Veríssimo, J. M. C. (2014). Digital marketing and social media: Why bother? *Business Horizons*, *57*(6), 703–708.

Undang-Undang

Peraturan Pemerintah no 82 tahun 2012 tentang Penyelenggaraan Sistem dan Teransaksi Elektronik

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-undang no 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik

PermenKominfo no 10 tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik Instansi Penyelenggara Negara