

KORELASI KEJAHATAN SIBER DENGAN PERCEPATAN DIGITALISASI DI INDONESIA

¹Sindy Ariyaningsih, ²A. Ari Andrianto, ³Adri surya Kusuma, ⁴Rezi
Universitas Duta Bangsa Surakarta, Surakarta, Indonesia
rezi@udb.ac.id

DOI:

Submit: 23-Februari-2023

Diterima: 30-Maret-2023

Dipublikasikan 30-Mei-2023

Abstract

In the rapidly evolving digitalization era in Indonesia, cybercrime has become an increasingly relevant and pressing issue. With the acceleration of digitalization in various sectors, including communication, business, and government, the threat of cybercrime has also significantly increased. The objective of this research is to analyze the correlation between cybercrime and the acceleration of digitalization in Indonesia. This research utilizes secondary data analysis, such as cybercrime reports, digitalization statistics, and relevant case studies. It also employs a qualitative approach to analyze the factors contributing to the correlation between cybercrime and the acceleration of digitalization in Indonesia. The findings of this research indicate a significant correlation between cybercrime and the acceleration of digitalization in Indonesia. Firstly, the growing number of internet users and the utilization of digital technology contribute to an increased potential for cybercrime attacks. Secondly, the growth of e-commerce and online transactions elevates the risks of fraud and data theft. Thirdly, the lack of cybersecurity awareness among digital users exacerbates the situation. Furthermore, other factors influencing the correlation between cybercrime and the acceleration of digitalization in Indonesia include the lack of adequate policies and regulations to address cybercrime, insufficient technical capabilities to combat cyber attacks, and a low level of collaboration between the public and private sectors in confronting cyber threats. This research provides several policy recommendations to mitigate the negative impact of cybercrime in the context of digitalization acceleration in Indonesia. These recommendations include enhancing cybersecurity awareness among the public, improving technical capacities to counter cyber attacks, strengthening collaboration between the public and private sectors, and developing better policies and regulations to address cybercrime.

Keywords: Cybercrime, Digitalization, Indonesia, Cybersecurity Awareness, Regulations

Abstrak

Dalam era digitalisasi yang semakin berkembang di Indonesia, kejahatan siber menjadi isu yang semakin relevan dan mendesak. Seiring dengan percepatan digitalisasi di berbagai sektor, termasuk komunikasi, bisnis, dan pemerintahan, ancaman kejahatan siber juga meningkat secara signifikan. Tujuan penelitian ini adalah untuk menganalisis korelasi antara kejahatan siber dengan percepatan digitalisasi di Indonesia. Metode yang digunakan dalam penelitian ini melibatkan analisis data sekunder, seperti laporan kejahatan siber, statistik digitalisasi, dan studi kasus yang relevan. Penelitian ini juga menggunakan pendekatan kualitatif untuk menganalisis faktor-faktor yang berkontribusi pada korelasi antara kejahatan siber dan percepatan digitalisasi di Indonesia. Hasil penelitian menunjukkan adanya korelasi yang signifikan antara kejahatan siber dengan percepatan digitalisasi di Indonesia. Pertama, semakin banyaknya pengguna internet dan penggunaan teknologi digital berkontribusi pada peningkatan potensi serangan kejahatan siber. Kedua, pertumbuhan e-commerce dan transaksi online meningkatkan risiko penipuan dan pencurian data. Ketiga, kurangnya kesadaran keamanan siber di kalangan pengguna digital juga menjadi faktor yang memperparah situasi. Selain itu, faktor-faktor lain yang mempengaruhi korelasi antara kejahatan siber dan percepatan digitalisasi di Indonesia termasuk kurangnya kebijakan dan regulasi yang memadai dalam menangani kejahatan siber, kurangnya kemampuan teknis dalam melawan serangan siber, dan rendahnya tingkat kerjasama antara sektor publik dan swasta dalam menghadapi ancaman kejahatan siber. Penelitian ini menghasilkan beberapa rekomendasi kebijakan untuk mengurangi dampak negatif kejahatan siber dalam konteks percepatan digitalisasi di Indonesia. Rekomendasi tersebut meliputi peningkatan kesadaran keamanan siber di kalangan masyarakat, peningkatan kapasitas teknis dalam melawan serangan siber, penguatan kerjasama antara sektor publik dan swasta, serta pengembangan kebijakan dan regulasi yang lebih baik dalam menangani kejahatan siber.

Kata Kunci: Kejahatan Siber, Digitalisasi, Indonesia, Kesadaran Keamanan, Regulasi

PENDAHULUAN

Era yang sekarang dikenal sebagai globalisasi pada dasarnya dimulai pada awal 1900-an, ketika revolusi transportasi dan elektronik mulai menyebar dan mempercepat perdagangan antar negara. Pertumbuhan dan kecepatan lalu lintas barang dan jasa juga berkembang pesat ide-ide modern seperti negara, konstitusi, nasionalisme, kapitalisme, demokrasi, sekularisme, serta globalisasi industri dan perusahaan media (Sembiring 2012).

Perkembangan teknologi pada masa ini mengubah struktur masyarakat dari masyarakat yang terstruktur lokal menjadi global (Raodia 2019). Karena kehadiran teknologi informasi yang berkembang pesat. Perkembangan teknologi informasi saat ini yang dipadukan dengan media dan komputer, memunculkan alat baru yang disebut internet. Keberadaan internet melahirkan paradigma baru dalam kehidupan manusia. Dalam kehidupan, hal-hal berubah dari nyata (nyata) ke realitas baru, yaitu maya (virtual). Realitas lain ini sering dikaitkan dengan internet dan ruang siber.

Kecanggihan teknologi informasi di zaman ini memang sangat bermanfaat bagi masyarakat. Kelebihan komputer dalam hal kecepatan dan ketepatan dalam bekerja, yaitu dapat mengurangi jumlah pekerja, biaya dan memperkecil kemungkinan terjadinya kesalahan, membuat orang semakin bergantung pada komputer. Namun konsekuensi negatif dapat terjadi jika ada bug pada perangkat keras komputer yang menyebabkan kerusakan besar pada pengguna atau pihak yang berkepentingan. Kesalahan yang disengaja menyebabkan penyalahgunaan komputer sebagai alat kejahatan bahkan perang modern.

Perkembangan informatika kontemporer, baik berupa internet maupun media sejenis lainnya, membawa berbagai konsekuensi. Perkembangan teknologi

informasi memiliki dampak positif dan negatif. Dari pemanfaatan teknologi informasi khususnya internet kita mendapatkan banyak peluang, dan tidak dapat dipungkiri bahwa teknologi informasi khususnya internet dapat digunakan untuk melakukan kejahatan yang awalnya hanya bersifat pengakuan, seperti pencurian, penipuan, ancaman, informasi hoax, dll. Media komputer dengan risiko yang sangat kecil untuk disadap.

Perkembangan dunia Internet di Indonesia telah mencapai tahap yang sedemikian pesat sehingga tidak heran jika di setiap sudut kota terdapat banyak warnet yang menawarkan berbagai layanan Internet. Pada awalnya, beberapa pengamat komputer meramalkan kematian Internet disekitar tahun 1980 karena hanya dapat bertukar informasi satu arah pada saat itu. Namun di masa depan ternyata prediksi itu salah, dan bahkan sekarang menjadi kebutuhan konstan akan informasi. Namun, keindahan Internet tidak seindah namanya, yang menjanjikan untuk menyediakan berbagai informasi di mana saja di dunia, karena lebih sering ditemukan berbagai jenis kejahatan nyata di sana. Kejahatan yang terjadi di internet biasa disebut dengan kejahatan siber. Ancaman kejahatan siber yang merupakan bentuk ancaman perang era modern atau non militer yang dapat memicu terjadinya disintegrasi bangsa melalui motif kepentingan individu atau kelompok tertentu.

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia di seluruh dunia. Selain itu, perkembangan teknologi informasi telah membuat dunia menjadi tak terbatas dan menyebabkan perubahan sosial yang besar begitu cepat (Rosana 2010). Teknologi informasi saat ini menjadi pedang bermata dua karena selain berkontribusi pada peningkatan

kesejahteraan, kemajuan dan peradaban manusia, juga merupakan arena yang efektif untuk kegiatan ilegal.

Berdasarkan uraian di atas, penulis tertarik untuk meneliti penggunaan alat bukti digital atau elektronik yang terdapat dalam Undang-Undang Informasi dan Perdagangan Elektronik Nomor 19 Tahun 2016 dan Perpres Nomor 3 Perubahan Undang-Undang Nomor 11 Tahun 2021 di lapangan. informasi dan perdagangan elektronik. kelompok kerja untuk mempercepat dan memperluas digitalisasi regional. Untuk itulah penulis menulis peraturan perundang-undangan dalam bentuk skripsi yang berjudul “Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi di Indonesia”.

METODE PENELITIAN

Dalam penelitian ini, digunakan metode kombinasi antara analisis data sekunder dan pendekatan kualitatif. Melalui analisis data sekunder, peneliti mengumpulkan berbagai data terkait kejahatan siber dan digitalisasi di Indonesia. Data tersebut meliputi laporan kejahatan siber dari lembaga yang berwenang, statistik mengenai pertumbuhan pengguna internet dan adopsi teknologi digital, serta studi kasus yang relevan. Analisis data sekunder ini memberikan pemahaman awal tentang gambaran umum korelasi antara kejahatan siber dan percepatan digitalisasi di Indonesia.

Selain itu, metode pendekatan kualitatif juga digunakan dalam penelitian ini. Melalui wawancara dengan para ahli keamanan siber, perwakilan lembaga penegak hukum, pengusaha di sektor digital, dan pemangku kepentingan lainnya, peneliti dapat memperoleh perspektif langsung mengenai korelasi tersebut. Wawancara ini memberikan

pemahaman yang mendalam tentang faktor-faktor yang mempengaruhi korelasi antara kejahatan siber dan percepatan digitalisasi di Indonesia.

Selain wawancara, peneliti juga melakukan analisis dokumen terkait, seperti kebijakan dan regulasi terkait kejahatan siber, laporan riset, dan publikasi akademik. Analisis dokumen ini memberikan pemahaman yang lebih mendalam tentang isu-isu terkait dan implikasi kejahatan siber dalam konteks percepatan digitalisasi di Indonesia.

Data yang diperoleh dari analisis data sekunder dan pendekatan kualitatif ini kemudian dianalisis secara komprehensif. Peneliti melakukan analisis terhadap data-data tersebut untuk mengidentifikasi korelasi antara kejahatan siber dan percepatan digitalisasi di Indonesia. Hasil analisis tersebut digunakan untuk merumuskan rekomendasi kebijakan yang relevan dalam menghadapi tantangan kejahatan siber di era digitalisasi.

Melalui penggabungan metode ini, penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang hubungan antara kejahatan siber dan percepatan digitalisasi di Indonesia, serta faktor-faktor yang mempengaruhinya.

HASIL PENELITIAN

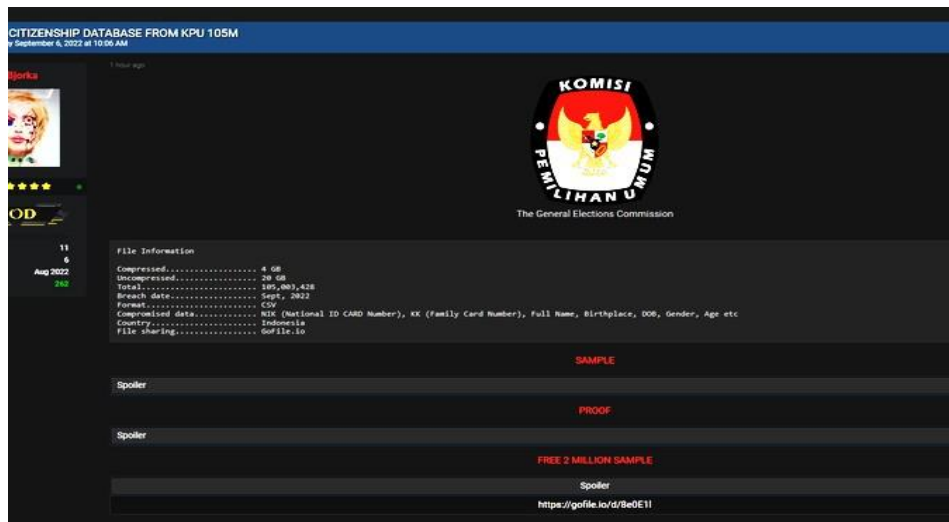
Indonesia juga telah dipengaruhi oleh insiden keamanan dunia maya global seperti ransomware coronavirus, malware Covidlock, peretasan Border Gateway Protocol, kerentanan router Draytek Vigor, eksekusi kode jarak jauh dari beberapa versi produk sistem operasi Windows, kerentanan eksekusi kode arbitrer di semua operasi Google Android. sistem, untuk menggunakan produk Solar Winds Orion Platform.



Gambar 01. Data serangan siber di Indonesia bulan Desember 2021.

Masa pandemi juga menjadi sasaran empuk bagi para peretas, yang terus berupaya menembus keamanan sistem perusahaan akibat tingginya penggunaan internet, di mana hampir semua orang bekerja dari rumah. Dikutip BSSN, Top Attacks Maret 2020, Terjadi 22 Serangan siber berlatar belakang masalah pandemi COVID-19, serangan ini diantaranya HawkEye Reborn Trojan, Blackwater

Malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, Ransomware Netwalker, Trojan Perbankan Cerberus, Malware Ursnif, Spyware Adobot, Trojan Pengunduh Metasploit, Spyware Projectspy, Trojan Perbankan Anubis, Adware, Iklan Tersembunyi (Android), Spyware AhMyth, Metasploit, Bot Xerxes, dan Pelacak atau tracker Covid19.



Gambar 02. Contoh kebocoran data yang dilakukan oleh Bjorka / Hacker

1. Jenis Serangan Siber

a. Cyber Crime

Dalam praktik cyber crime atau kejahatan siber, pelaku melakukan akses ilegal seperti transmisi ilegal atau manipulasi data untuk tujuan tertentu, di antaranya menciptakan gangguan dan mencari keuntungan finansial, bisa dilakukan seorang diri atau melibatkan sekelompok orang. Para pelaku cyber crime tentu adalah orang yang sudah ahli dalam berbagai teknik hacking, bahkan tak jarang sebuah aksi cyber crime dilakukan dari berbagai tempat berbeda di waktu bersamaan. Banyak contoh aksi cyber crime yang masih terjadi, seperti pencurian identitas (identity theft), penipuan/pembobolan kartu kredit (carding), memata-matai target tertentu (cyber espionage), dan lain-lain.

b. Cyber Warfare

Perkembangan teknologi informasi dan komunikasi memberi banyak kemudahan dalam menjalankan aktivitas pemerintahan, namun melahirkan ancaman baru yang berdampak bagi kestabilan kedaulatan suatu negara juga, yaitu cyber warfare. Cyber warfare merupakan perkembangan dari cyber attack dan cyber crime. Cyber warfare dapat diartikan sebagai perang di dalam cyber space, namun di dalam cyber warfare terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya.

Cyber warfare merupakan bentuk operasi siber (cyber operations) secara menyerang atau bertahan, yang dilakukan dengan tujuan untuk membuat cedera atau

kematian orang atau kerusakan atau kehancuran objek sasaran atau target operasi (Suharto and Maria Novita Apriyani 2021). Media utama yang digunakan di dalam cyber warfare adalah komputer dan internet, objek yang diserang dalam cyber warfare bukan merupakan wilayah fisik, wilayah teritorial ataupun wilayah geografis, namun objek dalam cyberspace yang dikuasai oleh suatu negara. Salah satu contoh kasus cyber warfare yaitu kasus antara Amerika Serikat dengan Iran di tahun 2008 dimana Amerika Serikat merusak sistem sentrifugal Pembangkit Listrik Tenaga Nuklir milik Iran.

c. Cyber Terrorism

Merupakan aktivitas sejumlah jaringan atau kelompok teroris yang bertujuan untuk mengganggu keamanan sosial, politik, dan ekonomi suatu negara dengan memanfaatkan kekuatan teknologi internet. Misalnya seperti menyerang website resmi pemerintah, melakukan sadap jaringan komunikasi strategis politik, mencuri sumber data elektronik perbankan, dan sebagainya. Aktivitas siber ini sangat berbahaya karena dapat menyebabkan kepanikan dan ketakutan skala besar.

2. Contoh Kejahatan Siber

a. Hoax

Media sosial menjadi media media paling diminati dalam mengakses suatu informasi. Selain itu, kecepatan dan kemudahan, serta konten dari pengguna menjadikan media sosial sebagai media yang paling banyak menyebarkan hoax. Penyebaran berita hoax ini sangat meresahkan masyarakat, dampaknya tidak hanya

terjadi kegaduhan di tengah-tengah masyarakat, tetapi juga dapat merusak (destruksi) kualitas demokrasi di Indonesia, bahkan berpotensi mengakibatkan perpecahan (disintegrasi) bangsa dengan penggiringan pola pikir dan opini publik atau masyarakat. Dengan transformasi informasi digital yang begitu cepat saat ini dan kerentanan isu hoax.

b. Cyber Attack

Beberapa metode yang umum digunakan oleh pelaku kejahatan cyber attack yang

menjadi ancaman keamanan siber adalah:

1) **Malware (Malicious software)**

Malware adalah salah satu ancaman cyber paling umum, berbentuk software yang dibuat untuk mengganggu atau merusak computer pengguna. malware sering sekali menyebar melalui lampiran email atau unduhan yang Nampak sah, beberapa malware yang umum dikenal yaitu :

Virus	program yang mereplikasi diri, menempel pada file bersih dan menyebar seluruh system computer pengguna
Trojan	Sejenis malware yang menyamar sebagai perangkat lunak yang sah. penjahat cyber menipu pengguna agar mengunggah trojan ke computer mereka untuk mengumpulkan data atau menyebabkan kerusakan
Spyware	program ini secara diam merekam apa yang dilakukan pengguna, sehingga penjahat dunia maya dapat mengguakan informasi ini. Misal digunakan untuk menangkap detail kartu kredit
Ransomware	Malware yang mengunci file dan data pengguna, dengan ancaman akan mempublikasikan, menghapus, atau menahan akses pengguna ke data pribadi yang penting kecuali pemilik data membayar tebusan.
Adware	perangkat lunak periklanan yang dapat digunakan untuk menyebarkan malware
Botnet	merupakan software yang bekerja secara otomatis (seperti robot) dalam menyebarkan dirinya ke sebuah host secara diam-diam dan menunggu perintah dari botmaster. Botnet sudah menjadi suatu bagian penting dari keamanan jaringan internet, karena sifatnya yang tersembunyi pada jaringan server internet.

2) **Social Engineering**

Social engineering adalah serangan yang didasari oleh interaksi manusia, dilakukan dengan manipulasi pengguna untuk memberikan informasi sensitive seperti password.

3) **Injeksi SQL**

Injeksi SQL (Structured Query Language) jenis ancaman cybersecurity yang

digunakan untuk mengambil kendali dan mencuri data dari pusat data. Pelaku biasanya memanfaatkan kerentanan dalam aplikasi basis data untuk memasukan perintah atau program kedalam basis data melalui pernyataan SQL.

4) **E-mail Spam dan Phising**

Merupakan kegiatan penipuan yang biasanya hadir

melalui email, pelaku akan mengirimkan email ke pengguna yang mirip dengan sumber terpercaya, dengan usaha fake login pada situs palsu yang menyerupai situ aslinya. Dimana sasaran metode ini adalah mencuri data sensitive seperti nomor keamanan kartu kredit (CVC), password dan informasi penting lainnya

5) Ancaman Domain Name

Asset yang berharga karena dapat diperjual belikan, disewa, dapat menjadi situs pemasang iklan sehingga menjadi sumber keuangan, bahkan dapat dijamin.

6) Dos (Denial of Service)

Metode kejahatan siber ini mencegah system computer memenuhi permintaan akses yang pengguna yang berhak atau yang berkepentingan tidak dapat menggunakan layanan tersebut. misalnya membanjiri jaringan dan server dengan trafik sehingga pengguna yang sudah terkoneksi didalamnya mengalami hilang koneksi.

3. Upaya Pemerintah Dalam Keamanan Siber

a. Capacity Building

program pelatihan dan pengembangan keamanan siber dilaksanakan berkoordinasi dengan kelompok kerja Pusat Operasi Pertahanan Siber. Selain itu, perlu adanya pengembangan sumber daya manusia tentang pentingnya keamanan siber untuk meningkatkan pemahaman tentang langkah-langkah pencegahan untuk memerangi semua kejahatan siber. Penataan ulang sistem

pertahanan berbasis cyber defense dan cyber security, yang tentunya membutuhkan persiapan yang matang dan sistematis dengan dukungan berbagai pihak. Sinergi dalam memerangi ancaman siber sangat penting dan diperlukan bagi Indonesia. Melalui sinergi dan komunikasi, koordinasi, jejaring dan kerja sama teknis, perlu diciptakan komunitas keamanan siber yang mampu menangkal, mendeteksi, memerangi, dan mencegah berbagai kemungkinan serangan dini ancaman siber untuk memperkuat keamanan dan ketahanan nasional. Operasi

BSSN saat ini dikritik karena tumpang tindih fungsi dengan institusi seperti Kementerian Komunikasi dan Informatika, Satuan Kejahatan Siber Polri dan Pusat Operasi Siber Kementerian Pertahanan. Ke depan, Indonesia harus mempercepat penerapan UU Keamanan Siber untuk menciptakan landasan hukum. Keberadaan undang-undang tersebut juga dapat mendorong strategi keamanan siber nasional yang komprehensif untuk lebih mendefinisikan fungsi BSSN. Oleh karena itu, sangat penting untuk menyelaraskan strategi keamanan siber dengan transformasi digital menjadi solusi keamanan berlapis (Sudarmadi and Runturambi 2019). Unit kerja, baik tim IT maupun tim bisnis, berada di lantai satu. Persyaratan keamanan, kesadaran keamanan informasi, kemampuan untuk merancang solusi yang aman dan pada saat yang sama menawarkan pengalaman yang menyenangkan. Tim manajemen risiko dan kepatuhan berada di lantai dua. Tim ini harus memiliki pandangan

yang komprehensif dan terkini tentang risiko keamanan siber untuk dibahas bersama. Di lantai tiga, ada grup audit yang menentukan apakah kontrol keamanan siber memadai atau tidak dan apakah perlu ditingkatkan. Tim audit ini harus memiliki keterampilan dan keahlian yang memadai untuk merespons risiko keamanan dunia maya saat ini. Yakni, kemampuan mengontrol keamanan cloud, pengembangan agile dan lain-lain.

Mengingat pentingnya keamanan siber, sangat mendesak untuk memperkuat lembaga yang bertanggung jawab atas koordinasi kegiatan, jika perlu dengan dukungan penuh dari semua pihak. Badan koordinasi harus terdiri dari orang-orang yang memiliki integritas dan kompetensi yang tinggi. Di tingkat operasional, setiap sektor harus memiliki tim tanggap darurat sendiri yang menangani insiden di sektornya dan yang peran dan tanggung jawabnya didefinisikan dengan jelas.

b. UU Tindak Pidana Siber

Pemerintah telah menerbitkan UU Informasi Teknologi Elektronik (ITE) yang dimaksudkan untuk mencegah dan meminimalisir upaya-upaya kejahatan pada dunia ITE yang mana dapat berimbas pada kerugian, kejahatan nyata dalam aplikasinya, keguncangan sosial dan bahaya disintergrasi bangsa. Beberapa penjelasannya adalah sebagai berikut:

1) Pasal 27 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan atau mentransmisikan dan/atau

membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.

- 2) Pasal 28 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
- 3) Pasal 29 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Cyber Stalking).
- 4) Pasal 30 UU ITE tahun 2008 ayat 3: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (cracking, hacking, illegal access).
- 5) Pasal 33 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.
- 6) Pasal 34 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki.

- 7) Pasal 35 UU ITE tahun 2008: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik (Phising atau penipuan situs).
- 8) Peraturan Menteri Kominfo No 4 Tahun 2016: Mengatur sistem manajemen pengamanan informasi.

4. Kerjasama

Masalah keamanan siber sangat kompleks, membutuhkan pendekatan multidimensi. Oleh karena itu, penerapan prinsip multi-stakeholder menjadi sangat penting untuk meningkatkan tata kelola keamanan siber. Tanpa kerjasama para pemangku kepentingan (dari lembaga publik hingga sektor swasta, universitas dan masyarakat sipil), masalah penyelesaian masalah terkait keamanan siber akan tetap berat sebelah dan tidak lengkap. Yang dibutuhkan adalah mekanisme partisipatif yang dapat memvalidasi keputusan dan mempertimbangkan kepentingan nasional dan populasi yang terkena dampak melalui badan yang menaunginya seperti BSSN, BIN, atau kerjasama internasional dalam peningkatan kapasitas keamanan siber.

5. Upaya Individu Dalam Keamanan Siber

a. Pentingnya Sadar Kebenaran Informasi

Selain bermanfaat untuk pergaulan semata, ternyata medsos dapat dijadikan sebagai media untuk menyebarkan informasi atau pesan yang mengandung fitnah dan

diragukan kebenarannya (Hoax) sehingga dapat membangkitkan rasa permusuhan terhadap sesama dan terjadinya disintegrasi bangsa. Beberapa hal yang dapat dilakukan untuk meminimalisir terjadinya hoax yang meluas yang dapat dilakukan oleh setiap individu diantaranya adalah:

- 1) Melakukan cek sumber informasi atau berita
- 2) Melakukan cek kelengkapan informasi
- 3) Mencermati fakta
- 4) Jangan termakan judul (provokatif)
- 5) Memeriksa keaslian foto atau video
- 6) Memperhatikan tanggal artikelnya
- 7) Menghindari sharing berita berlebihan

b. Pentingnya Sadar Keamanan Informasi

Sumber daya manusia merupakan satu unsur yang terpenting dalam memastikan terlaksananya keamanan siber, dengan dukungan dari kebijakan-kebijakan yang ditetapkan pemerintah. Pengetahuan dan kesadaran pribadi akan kebenaran dan keamanan informasi perlu di pelihara demi terhindar dari devide et impera modern atau hoax dan kejahatan digital. Berbicara kejahatan dalam dunia siber, semua bisa terjadi dengan pelaku yang sama dengan 1 akun, 1 pelaku banyak akun, 1 institusi, 1 negara, bahkan 2 negara yang bermusuhan menjadi bekerja untuk menyerang target yang sama dengan segala kepentingan pribadinya yang dapat memicu isu-isu menuju disintegrasi bangsa di semua unsur.

c. Peran Dan Peningkatan SDM

Pada umumnya masyarakat Indonesia sudah cukup mengenali tentang technology risk tetapi kurang begitu memahami tentang perlindungan

konsumen. Dimana kondisi corporate di Indonesia rata-rata berhadapan langsung dengan konsumen sebelum ke pemerintah. Sehingga konsumen memiliki kekuatan yang kurang apabila terjadi permasalahan hingga ketika sebuah corporate yang menyelenggarakan sistem elektronik mengalami kebocoran data. Regulasi ini sudah mulai dibenahi oleh pemerintah kita saat ini. Namun tentunya tanpa dukungan pakar yang menekuni atau meningkatkan keilmuan di bidang tersebut akan sulit dicapai karena percepatan digital di segala bidang akan selalu berhubungan dengan big data yang rentan dengan kejahatan-kejahatan siber. Tanpa atau kurangnya ahli dibidang tersebut, tentunya adalah masalah besar bagi terciptanya keamanan yang substantif.

Kolaborasi dengan teknologi juga dapat menjadi problem solving yang di dapat dikembangkan oleh para ahli IT untuk memerangi kejahatan non militer ini. IoT dan AI dengan segala inovasi sistem yang dapat dibangun di dalamnya dengan pengembangan terstandarisasi dan terstrukturisasi akan melawan dan dapat meminimalisir segala kemungkinan buruk yang bisa terjadi dalam ruang lingkup digital yang mulai melebur menjadi satu dalam ruang nyata seperti saat ini yang sedang berlangsung.

CONCLUSION

Percepatan digitalisasi sedemikian pesat, hal ini memberikan kemudahan di

segala aspek kegiatan masyarakat di Indonesia. Namun di dalam ruang digital tersebut perlu di waspadi banyaknya pemicu disintegrasi bangsa dengan segala bentuk kejahatan modern melalui internet yang bisa saja terjadi pada pengiriman informasi atau komunikasi yang tidak jelas kebenarannya atau bahkan menyerang secara terang-terangan yang biasa dikenal dengan kejahatan atau serangan siber. Dalam ruang tanpa batas dan jenis serangan yang begitu banyak, skala kejahatan siber dapat dilakukan dengan pelaku yang sama dengan 1 akun, 1 pelaku banyak akun, 1 institusi, 1 negara, bahkan 2 negara yang bermusuhan menjadi bekerja untuk menyerang target yang sama dengan segala kepentingan pribadinya. Sehingga sebuah kemudahan dari digitalisasi juga perlu di imbangi dengan semakin kuatnya keamanan siber.

Pemerintah telah berupaya dalam meminimalisir segala bentuk kejahatan siber di saat percepatan dan pemerataan digitalisasi di Indonesia terjadi dengan capacity building, pembentukan UU tindak pidana siber, dan bekerja sama dengan badan atau organisasi yang memiliki kompetensi di dalam keamanan siber baik nasional maupun internasional.

Upaya pemerintah dalam menjaga percepatan digitalisasi terhadap serangan kejahatan siber ini tentunya membutuhkan dukungan dari setiap individu masyarakat. Hal ini dapat dilakukan oleh masing-masing individu dengan menyikapi suatu informasi secara benar, memiliki kesadaran pribadi akan pentingnya keamanan informasi, peningkatan sumber daya manusia, serta pemanfaatan teknologi informasi dilakukan secara bijak..

REFERENCES

- Dawwas, Rizal. 2021. "Upaya Penanggulangan Disintegrasi Nasional Dalam Menjaga Persatuan Indonesia." *Jurnal Hukum* 1(1): 20–

26.
<http://jurnal.umpwr.ac.id/index.php/eksaminasi/article/view/1186>.
- Gani, Alcianno G. 2014. "Cybercrime (Kejahatan Berbasis Komputer)." *Jurnal Sistem Informasi Universitas Suryadarma* 5(1): 16–29.
- Junaidi, Fadhli. 2021. "Transformasi Digital, Pelayanan Publik Di Masa Pandemi." *Ekasakti Education Journal* 1(2): 1–10.
- Raodia, Raodia. 2019. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah dan Hukum* 6(2): 39.
- Rosana, Anita Septiani. 2010. "Kemajuan Teknologi Informasi Dan Komunikasi Dalam Industri Media Di Indonesia." *Gema Eksos* 5(2): 146–48.
<https://www.neliti.com/id/publications/218225/kemajuan-teknologi-informasi-dan-komunikasi-dalam-industri-media-di-indonesia>.
- Sembiring, Ivan Giovani. 2012. "Tinjauan Yuridis Tentang Pengaturan Dan Kependudukan Internet Protokol Sebagai Alat Bukti Dalam Tindak Pidana Kejahatan Mayantara (Cyber Crime)." [http://repository.umsu.ac.id/handle/123456789/8050%0Ahttp://repository.umsu.ac.id/bitstream/123456789/8050/1/SKRIPSI WIRA FHADLY.pdf](http://repository.umsu.ac.id/handle/123456789/8050%0Ahttp://repository.umsu.ac.id/bitstream/123456789/8050/1/SKRIPSI%20WIRA%20FHADLY.pdf).
- Sudarmadi, Damar Apri, and Arthur Josias Simon Runturambi. 2019. "Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 2(2): 157–78.
<http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/28>.
- Suharto, Miko Aditiya, and Maria Novita Apriyani. 2021. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum* 17: 98–107.