COMSERVA
JURNAL PENELITIAN DAN PENGABDIAN MASYARAKAT
Volume 2 No. 11, Maret 2023 (2477-2486)
e-ISSN: 2798-5210
p-ISSN: 2798-5652

Lingkup Dunia Cyber di Indonesia

Cyber World Scope in Indonesia

Desri Amanda Firdayani Nasution, Ria Septiana, Widya Syaputri, Nurbaiti
Universitas Islam Negeri Sumatera Utara

*Email: desriamanda22@gmail.com, septianaria3667@gmail.com, saputriw568@gmail.com, nurbaiti@uinsu.ac.id
Correspondence: Desri Amanda Firdayani Nasution

DOI: 10.36418/comserva.v2i11.653

Histori Artikel
Diajukan : 03-02-2023
Diterima : 18-03-2023
Diterbitkan : 25-03-2023

ABSTRAK

Di jaman sekarang perkembangan teknologi semakin maju, banyak yang yang memanfaatkan internet sebagai salah satu alat atau ruang berkomunikasi dengan orang lain. Namun, dengan kemajuan teknologi dan internet juga tidak hanya memberikan dampak positif, melainkan terdapat juga sisi negatifnya, yaitu banyak juga dari orang-orang yang melakukan pengancaman dari internet atau yang biasa disebut juga dengan Cyber crime. Cyber crime adalah serangan yang dilakukan melalui teknologi internet. Serangan cyber juga menjadi salah satu serangan yang sering terjadi di dunia, salah satunya indonesia. Untuk tahun 2022 saja sudah lebih dari 700 juta serangan cyber yang dilakukan. Berdasarkan dari data yang didapat, penelitian ini termasuk dalam kategori penelitian kualitatif. Penelitian kualitatif merupakan penelitian yang pada dasarnya cara untuk memahami fenomena dengan cara memperoleh data dari penelitian berupa data atau aktivitas yang dilihat dari observasinya. Penelitian ini dilakukan untuk menguji seberapa banyak serangan yang dilakukan oleh cyber terhadap dunia termasuk negara indonesia. Cybersecurity juga dilakukan pada tahap ini agar tindakan pencurian data tidak terjadi yang dapat merugikan negara dan orang lain juga.

Kata Kunci: Teknologi; internet; Cybercrime; Cybersecurity

ABSTRACT

In this day and age, technological developments are increasingly advanced, many use the internet as a tool or space to communicate with others. However, with the advancement of technology and the internet, it also not only has a positive impact, but there is also a negative side, namely that there are also many people who make threats from the internet or what is also known as Cybercrime. Cybercrime is an attack carried out through internet technology. Cyber attacks are also one of the most common attacks in the world, one of which is Indonesia. For 2022 alone, more than 700 million cyberattacks have been carried out. Based on the data obtained, this research is included in the category of qualitative research. Qualitative research is research that is basically a way to understand phenomena by obtaining data from research in the form of data or activities seen from observations. This research was conducted to test how many attacks are carried out by cyber against the world, including the country. Cybersecurity is also carried out at this stage so that data theft actions do not occur that can harm the country and others as well.

***Keywords**: Technology; Internet; Cybercrime; Cybersecurity*

PENDAHULUAN

Kehadirann internet telah menciptakan dunia baru berbasis komputer. Cyber sering terikat pada teknologi dari komputer dan internet (Idik Saeful Bahri, 2020). Dengan menggunakan internet, para pengguna dapat bebas menjelajahi cyberspace tanpa ada batasan dari negara. Menurut Howard Rheingold cyberspace merupakan sebuah ruang imajiner atau maya yang bersifat artifisal, dimana setiap orang melakukan aktivitas ataupun kegiatan yang biasa dilakukan dalam kehidupan sosial sehari-hari dengan cara yang baru (Utomo, 2017).

Pengaruh dari internet telah mendorong sebuah negara untuk mengembankan Teknologi yang lebih maju (Rohida, 2018). Namun menurut (Raodia, 2019) perkembangan internet yang pesat, dapat juga menimbulkan kejahatan digital (cyber crime).

Pada perkembangannya cyber crime merupakan suatu tindakan dengan penggunaan jaringan komputer yang mengarah pada tujuan kriminal tinggi yang menyalahgunakan kemudahan teknologi (Dermawan & Akmal, 2020). Nah, cyberspace yang bersifat global membuat cyber crime sulit untuk ditentukan ranah kuasanya.

Ancaman cyber dapat menjadi salah satu ancaman yang dapat merugikan negara, salah satunya pencurian data informasi. Salah satu ancamannya terdiri dari serangan melalui virus, situs-situs resmi, para hacker dan kegiatan lainnya yang menjadi ancaman juga tantangan yang harus diwaspadai oleh lembaga pertahanan ataupun yang berwenang dalam menjaga keamanan siber nasional (Simarmata et al., 2022).

Tinjauan Teoritis

Ruang lingkup cyber yang sering menjadi masalah yaitu cyber crime dan cyber security yang berfokus pada serangan teknologi yang sering dilakukan oleh orang-orang yang tidak bertanggung jawab yaitu kasus penipuan yang menggunakan internet sebagai sarana penipuan. Keamanan cyber (cyber security) dapat disimpulkan untuk menjaga dan melindungi dari serangan melalui cyberspace (hardware, software, computer network) (Budi et al., 2021). Keamanan cyber dapat digambarkan dari sisi kebijakan, pedoman, dan proses yang diperlukan untuk meminimalisir ancaman. Keamanan cyber terdiri dari insfrastruktur perangkat lunak dan keras.

Untuk itu pemerintah menerapkan, Undang undang nomor 11 tahun 2008 tentang internet & transaksi elektronik (ITE) Undang undang ini, yang telah disahkan dan diundangkan pada tanggal 21 april 2008 (Sidik, 2013), walaupun sampai dengan hari ini belum ada sebuah peraturan yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang undang cyber atau cyberlaw guna menjerat pelaku pelaku cybercrime yang tidak bertanggung jawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) atau lebih kita kenal dengan sebutan UU ITE telah berlaku sejak diundangkan pada tahun 2008. Sejak diberlakukan, UU ITE sudah mendapat banyak masukan dan aspirasi dari Lembaga Swadaya Masyarakat (LSM), akademisi, praktisi dan juga masukan dari masyarakat. Pemerintah melalui Kementerian Komunikasi dan Informatika telah menjawab masukan-masukan tersebut dengan melakukan revisi UU ITE dengan skema revisi terbatas, yang dimaksud dengan skema revisi terbatas adalah revisi yang difokuskan pada pasal-pasal tertentu sehingga tidak memberi tempat lagi untuk kriminalitas seperti yang diaspirasikan (Napitupulu et al., 2020). Revisi ini juga memberi wadah untuk memberikan perlindungan hukum, ekosistem yang adil bagi seluruh lapisan masyarakat.

Dengan adanya revisi UU ITE, pasal pencemaran nama baik yang awalnya adalah delik umum berubah menjadi delik aduan, maknanya hanya dapat diproses secara hukum jika dilaporkan oleh

korban atau seseorang yang merasa menjadi sasaran (Uttata, 2020). Selain perubahan itu, perubahan lain terkait pasal pencemaran nama baik yaitu diturunkannya ancaman hukuman yang semula maksimal 6 tahun menjadi 4 tahun. Dengan demikian tersangka pelaku pencemaran nama baik tidak akan ditahan karena dalam KUHP dijelaskan bahwa penahanan perlu dilakukan jika ancaman penjara di atas lima tahun.

Selain perubahan pada pasal pencemaran nama baik, revisi pada UU ITE ini juga menambahkan ketentuan mengenai *right to be forgotten* atau hak untuk dilupakan dengan menghapus konten informasi elektronik yang tidak benar berdasarkan keputusan pengadilan (Fitri, 2022). Mengutip pernyataan dari Juru bicara Kemenrian Komunikasi dan Informasi, Noor Iza bahwa penghapusan konten dilakukan untuk seluruh data di internet setelah dibuktikan di pengadilan karena bertujuan untuk membersihkan nama baik seseorang, "Agar konten-konten itu tidak dapat diakses, dikeluarkan dari sistem yang terbuka atau konten-konten itu dihapus". Tidak dapat di cari juga, jadi search engine harus menghilangkan dan juga server-server dan harus menutup konten-konten itu agar tidak dapat diakses".

Revisi UU ITE yang berlaku mulai 28 November 2016 ini mengharuskan warga Indonesia yang aktif menggunakan sosial media untuk lebih berhati-hati dalam mengekspresikan argumen mereka maupun ketika berbagi berita atau cerita dari halaman Facebook milik orang lain (Oksidelfa Yanto, 2021). Karena bila ada yang merasa menjadi korban atas pendapat kita atau cerita yang kita share maka orang tersebut dapat menuntut kita. Akan lebih baik bila kita belajar untuk membaca semua cerita atau berita sebelum kita bagikan di halaman Facebook milik kita.

METODE

Metode penelitian ini dibuat dalam jenis penelitian kualitatif berbasis tinjauan buku dan artikel. Penelitian Kualitatif adalah penelitian yang pada dasarnya merupakan cara ilmiah untuk memahami fenomena dengan cara memperoleh data dari penelitian berupa data atau aktivitas yang dilihat dari observasinya (Anggito & Setiawan, 2018).

Menurut Bogdan dan Taylor Metode penelitian kualitatif adalah, "prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis ataupun lisan dari orang-orang dan perilaku yang dapat diamati (Abrori, 2018). Dengan demikian pendekatan penelitian ini dapat diarahkan pada latar dan individu tersebut".

Dengan demikian metode pada penelitian kualitatif adalah metode penelitian yang dapat digunakan untuk meneliti kondisi objek yang alamiah dimana peneliti merupakan intrumen kunci atau peran penting, analisis data bersifat induktif dengan hasil penelitian yang lebih menekankan pada makna kejadian yang terjadi (Yulianah, 2022).

HASIL DAN PEMBAHASAN

Sistem pertahanan negara dapat terdiri dari ancaman militer dan ancaman non militer, salah satu contohnya yaitu serangan dari ancaman Cyber. Serangan cyber menjadi sangat serius, dilihat dari data Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII) terdapat 714.170.967 juta serangan Internet sepanjang tahun 2022 di Indonesia. Jenis serangan yang sering ditemukan yaitu serangan ransomware atau serangan yang meminta tebusan kepada pemilik data. Tingginya angka kejahatan dan peretas di bidang Internet ini menjadi ancaman di tengah masifnya pertumbuhan pengguna internet di Indonesia. Serangan cyber mengancam di berbagai sektor antara lain Pelayanan Publik, Ekonomi, Pertahanan, Keamanan, dan Energi. Pertahanan cyber tidak mengenal batas disuatu negara, karena serangan bisa datang dari dalam maupun dari luar negeri.

Keamanan dan manajemen data adalah konsep yang sangat penting dari E-security. Dalam unit ini berbagai konsep penting dibahas panjang lebar untuk pemahaman dan penerapan yang lebih baik di tempat yang tepat. Terutama konsep keamanan data, melindungi data sensitif, data sensitif browser, tata kelola data, penjelajah internet dan keamanan jaringan, peran window-Microsoft: membantu melindungi OC Anda, manajemen keamanan data, manajemen kualitas data perusahaan dan keamanan serta privasi data di kunci dan dibahas panjang lebar untuk memahami unit sepenuhnya.

Pencurian Identitas: kejahatan yang berkembang

Istilah pencurian identitas diciptakan pada tahun 1964. Namun, secara harfiah tidak mungkin untuk mencuri identitas istilah yang kurang ambigu merupakan manipulasi identitas atau peniruan identitas istilah yang cenderung kurang mengacu pada penempatan tanggung jawab pada orang yang ditiru dan yang cenderung lebih mengarah pada penempatan tanggung jawab yang tepat pada korban dan pelaku. Tipuan "Menentukan hubungan antara pelanggaran data dan pencurian identitas itu menantang, terutama karena korban pencurian identitas sering tidak tahu bagaimana informasi pribadi mereka diperoleh," dan pencurian identitas tidak selalu dapat dideteksi oleh masing-masing korban, menurut laporan yang dilakukan untuk FTC. Penipuan identitas sering terjadi tetapi tidak selalu merupakan konsekuensi dari pencurian identitas itu sendiri (Simbolon, 2019).

Pencurian identitas adalah salah satu kekhawatiran yang berkembang dalam kejahatan dunia maya di India saat ini. Menurut Norton Cybercrime Report 2011, secara global 431 juta orang dewasa mengalami kejahatan dunia maya pada tahun 2011 dan lebih dari 1 juta lebih orang dewasa menjadi korban setiap hari. Sesuai laporan, India dengan cepat muncul sebagai sasaran empuk untuk kejahatan dunia maya terorganisir dengan empat dari lima orang dewasa online telah menjadi korban pencurian identitas pada tahun 2011.

Pengaruh Terorisme Cyber Terhadap Infrastruktur Nasional/ Internasional

Maksud serangan terorisme cyber dapat berkisar dari gangguan ekonomi melalui gangguan jaringan dan sistem keuangan yang digunakan untuk mendukung serangan fisik hingga menimbulkan kebingungan lebih lanjut dan kemungkinan penundaan dalam respons yang tepat. Meskipun serangan siber telah menyebabkan kerugian yang sangat besar yakni berkisar miliaran dolar dan mempengaruhi kehidupan jutaan orang lainnya, kita belum menyaksikan implikasi dari serangan terorisme cyber yang benar-benar dahsyat.

Ada beberapa implikasi dari implikasi biaya langsung, antara lain:

1. Kehilangan penjualan selama gangguan
2. Waktu staf, penundaan jaringan, akses terputus-putus untuk pengguna bisnis
3. Peningkatan biaya asuransi karena litigasi
4. Hilangnya kekayaan intelektual – penelitian, penetapan harga, dll.
5. Biaya forensik untuk pemulihan dan litigasi
6. Hilangnya komunikasi penting pada saat darurat
7. Implikasi Biaya Tidak Langsung
8. Hilangnya kepercayaan dan kredibilitas dalam sistem keuangan kita
9. Hubungan yang ternoda & citra publik secara global
10. Hubungan mitra bisnis yang tegang – domestik dan internasional
11. Hilangnya pendapatan pelanggan di masa depan untuk individu atau kelompok perusahaan
12. Hilangnya kepercayaan pada pemerintah dan industri computer.

Strategi Menghadapi Ancaman Terorisme Dunia Maya

Berurusan dengan teroris dunia maya dan terorisme dunia maya membutuhkan rencana yang matang dan tersusun, serta kemauan untuk mengambil tindakan segera, sebaiknya sebelum peristiwa teroris terjadi. Berikut ini adalah pendekatan sederhana untuk keamanan cyber:

1. Lakukan apa pun untuk melindungi infrastruktur.
2. Berinvestasi untuk melindungi produk Anda.
3. Lindungi klien Anda, termasuk data pribadi mereka.

Pastikan infrastruktur Anda, baik itu komputer pribadi, media sosial, maupun akun online Anda atau stasiun saluran air bernilai miliaran dolar dilindungi. Mulai dari yang kecil. Pastikan semua kata sandi kuat dengan memasukkan huruf kapital dan huruf kecil, angka serta simbol dalam kombinasi yang tidak biasa. Investasikan pada produk yang meningkatkan keamanan sistem, seperti perlindungan malware dan deteksi virus, dan gunakan enkripsi guna membantu melindungi informasi pribadi klien Anda. Mengambil keamanan ke tingkat yang lebih tinggi, pertimbangkan untuk menyewa peretas etis untuk mencoba mendapatkan akses ke sistem Anda, dan segera menutup kerentanan apapun. Juga pertimbangkan pemantauan ancaman orang dalam untuk mengidentifikasi perilaku dan anomali dengan sistem Anda dan untuk membantu memenuhi tuntutan sumber daya manusia (SDM). Dibutuhkan banyak orang untuk melindungi organisasi secara memadai, sama seperti dibutuhkan banyak orang untuk menyelesaikan serangan cyber. Oleh karena itu, berpikirlah seperti teroris dunia maya untuk mengalahkan mereka di permainan mereka sendiri. Mereka menggunakan teknologi untuk mencapai tujuan teroris mereka, jadi ikuti dan gunakan teknologi etis untuk memerangi tindakan tidak etis dari mereka dan sebarkan keamanan sejauh mungkin di dalam organisasi Anda.

Terorisme Cyber Yaitu Kejahatan Cyber

Terorisme dunia maya juga jelas merupakan ancaman yang muncul. Kelompok teroris semakin paham komputer, dan beberapa mungkin memperoleh kemampuan untuk menggunakan serangan dunia maya untuk menimbulkan gangguan yang terisolasi dan singkat terhadap infrastruktur AS. Karena prevalensi alat peretas yang tersedia untuk umum banyak dari kelompok-kelompok ini mungkin sudah memiliki kemampuan untuk meluncurkan penolakan layanan dan serangan gangguan lainnya terhadap sistem yang terhubung ke Internet. Ketika teroris menjadi lebih pahamt tentang komputer, opsi serangan mereka hanya akan meningkat. (War on Terrorism, 2003) Inilah yang Robert Mueller, Direktur FBI, bersaksi pada 11 Februari 2003 di hadapan Senat AS dalam dengar pendapat tentang War On Terrorisme melawan Al-Qaeda dan organisasi teroris lainnya.

AS dan organisasi media global mengambil kesaksian ini dan mulai berspekulasi tentang kemungkinan serangan teroris Cyber skala besar. Sejauh ini, serangan seperti itu belum terwujud. Pada saat yang sama istilah yang sama, Cybercrime, digunakan untuk menggambarkan kegiatan kriminal di Internet seperti pencurian identitas, pelanggaran hak cipta dan penipuan bank, tetapi sering kali kedua istilah ini (Cybercrime dan Cyber terrorism) akhirnya digunakan secara bergantian dan maknanya, terutama bagi publik, menjadi kabur dan tidak jelas. Pemerintah, jaringan kebijakan dan media di seluruh dunia telah terlibat dalam upaya membangun pertahanan terhadap serangan Cyber, memberlakukan peraturan baru sambil mempertahankan suasana yang hampir mitologis atas ancaman dan risiko potensi Cybercrime dan serangan teroris Cyber. Karena jangkauan global Internet terus berkembang, pengaruhnya pada semua bidang usaha manusia online menjadi lebih luas lagi. Individu atau kelompok dapat mengeksploitasi anonimitas yang diberikan oleh dunia maya untuk terlibat dalam kegiatan ilegal atau terlarang yang bertujuan untuk mengintimidasi, membahayakan, mengancam, atau menimbulkan ketakutan bagi warga, komunitas, organisasi, atau negara. Jarak virtual dan fisik antara penyerang dan korban dan kesulitan dalam melacak kembali serangan ke individu meminimalkan

ancaman penangkapan yang melekat pada penyerang. Tetapi bagaimana aktivitas tersebut didefinisikan? Apa itu Cybercrime dan apa ciri-cirinya? Bagaimana seorang Cyberterrorist dapat diidentifikasi dan apa perbedaannya dari Cybercriminal? Sejauh ini, definisi Cybercrime dan Cyber terrorism dalam literatur, dokumen pemerintah, dan penggunaan sehari-hari sangat bervariasi, spesifik konteks dan sarat emosional, yang membuat wacana tentang subjek menjadi sulit. FBI sendiri telah menerbitkan tiga definisi berbeda tentang terorisme Cyber: "Terorisme yang memulai serangan terhadap informasi" pada tahun 1999, hingga "penggunaan alat Cyber" pada tahun 2000 dan "tindakan kriminal yang dilakukan dengan penggunaan komputer" pada tahun 2004 (Herman, 2019).

Cybercrime dan Cyber terrorism telah digunakan untuk menggambarkan tindakan online seperti:

1. Peretasan / Cracking topi hitam
2. Pelanggaran seks anak (pornografi dan dandanan)
3. Kejahatan di dunia maya
4. Aktivisme dunia maya / Hacktivisme
5. Penulisan virus dan malware
6. Penguntit dunia maya
7. Pencurian identitas / Penipuan
8. Transaksi keuangan ilegal / Pencucian uang
9. Pelanggaran hak cipta
10. Tindakan cyber bullying yang serius
11. Serangan penolakan layanan
12. Rogue bot-net

Cyber terorism biasanya memiliki arti yang lebih kuat daripada Cybercrime, menggambarkan tindakan yang memiliki karakteristik serupa dengan serangan terorisme dunia nyata, tapi tidak selalu (Ginting, 2018). Di sisi lain, Cybercrime sering digunakan sebagai istilah umum untuk menggambarkan aktivitas ilegal, berbahaya dan bermusuhan di Internet termasuk terorisme Cyber. Selain itu, istilah lain terkadang digunakan untuk menggambarkan tindakan online terlarang yang serupa, yang semakin memperumit masalah, dan penggunaannya biasanya bergantung pada konteks atau orang/organisasi yang menggunakannya. Misalnya, seorang juru bicara dalam militer kemungkinan akan menggunakan istilah Perang siber untuk menggambarkan tindakan daring yang bermusuhan antara dua negara atau tindakan terorisme yang berasal dari negara lain dan dimanifestasikan secara daring (bukan menggunakan istilah Terorisme dunia maya).

Sebelum mencoba mendefinisikan terorisme Cyber dan Cybercrime, kita harus merenungkan validitas kedua istilah tersebut. (Sarinastiti & Vardhani, 2017) berpendapat bahwa "Terorisme siber, apa pun itu, adalah istilah yang tidak berguna" dan dia percaya bahwa, "teroris akan menggunakan alat strategis apa pun yang mereka bisa" sehingga terorisme Cyber tidak lebih penting daripada bentuk lainnya. Argumen serupa dapat dibuat untuk Cybercrime, seperti (Loader & Thomas, 2013) mengatakan, "Cybercrime relatif tidak berarti dengan sendirinya karena merupakan konstruksi fiksi yang tidak memiliki titik acuan asli dalam hukum, ilmu pengetahuan atau tindakan sosial." Namun, istilah ini secara bertahap mendapatkan landasan dalam wacana hukum formal karena undang-undang baru di banyak negara seperti Australia (Cybercrime Act 2001), Nigeria (Draft Cybercrime Act), Amerika Serikat (Usulan Cybercrime Act 2007) dan Inggris (The Home Office memperkenalkan Strategi Kejahatan Dunia Maya pada Maret 2010) (Hooper et al., 2013). Lapisan kerumitan tambahan ditambahkan ketika kita melihat sistem hukum dari berbagai negara dan definisi mereka yang beragam

tentang tindakan melanggar hukum. Bukan hal yang aneh jika satu negara mendefinisikan sebagai tindak pidana hanya menjadi kesalahan perdata di negara lain. Masalah muncul ketika seseorang adalah penerima beritatentang serangan teroris Cyber di negara asing, yang hanya akan dicirikan sebagai upaya peretasan atau protes aktivitas Cyber di negaranya sendiri, begitupun sebaliknya. Dengan demikian, kemungkinan besar seseorang dapat menunjukkan perasaan takut, tidak aman, cemas, atau panik yang tidak beralasan, bersama dengan kebingungan umum mengenai cara menafsirkan berita. Kejahatan dunia maya dan terorisme dunia maya adalah dua ancaman yang kemungkinan akan terus menerus ada selama bertahun-tahun yang akan datang dan pastinya harus diatasi. Tetapi proses ini perlu dilakukan dengan cara yang akan memastikan pertumbuhan Internet secara inklusif dan terbuka, mempertahankan prinsip-prinsip dasar yang telah dibangun di atasnya. Salah satu isu utama adalah disambiguasi dari istilah Cybercrime dan Cyber terrorism. Badan-badan pemerintah, jaringan kebijakan, cendekiawan, media, dan orang-orang perlu dilibatkan dalam percakapan global yang akan membantu mengungkap kejahatan dunia maya dan menentukan apa yang dimaksud dengan kejahatan dunia maya dan bagaimana penjahat dunia maya harus ditangani. Terorisme dunia maya harus diasingkan dari kejahatan dunia maya dan ditentukan secara realistis, seperti apa kemungkinan bahaya dari tindakan teroris dunia maya dan sejauh mana kita sebagai masyarakat harus menghadapi efek tersebut. Setelah kedua istilah ini didefinisikan dengan jelas dan tidak ambigu, orang akan jauh lebih siap untuk menerima dan memahami berita dan kebijakan yang terkait, dan akan dapat terlibat dalam wacana yang bermakna tentang subjek tersebut. Ini akan membantu mengurangi ketakutan yang tidak beralasan sementara pada saat yang sama memungkinkan seseorang untuk membuat keputusan yang tepat ketika mempertimbangkan kebijakan baru yang diusulkan dengan menimbang pro versus kontra dan dampaknya pada berbagai tingkatan, jangka panjang dan jangka pendek, alih-alih menyerah pada rasa takut dan kehilangan privasi dan kebebasan online mereka untuk keamanan yang lebih baik.

Peran media (televisi, blog, outlet berita online, dan lainnya) sangat penting dalam proses mendidik publik dan terlibat dalam percakapan, karena mereka akan menjadi mediator dan kurator informasi dan wacana tentang masalah tersebut. Dengan demikian, pendekatan yang ringkas dan masuk akal, tanpa praktik ketakutan dan kejutan, harus diikuti. Karena ini adalah masalah internasional, pemerintah dan jaringan kebijakan di seluruh dunia harus berkumpul dan berdiskusi secara terbuka tentang apa yang lebih baik bagi warganya. Cendekiawan dan akademisi dapat memberikan keahlian yang berharga tentang masalah teknologi, psikologis, etika, dan lainnya, sambil menyoroti keraguan apa pun oleh mereka yang terlibat dalam proses tersebut. Orang-orang di komunitas lokal, keluarga, dan jejaring sosial mereka harus saling membantu dan melatih untuk meningkatkan tingkat literasi internet rekan-rekan mereka dan menyoroti keunggulan web. Tingkat literasi Internet yang lebih tinggi dapat membantu orang melindungi diri mereka sendiri lebih baik dengan mengambil langkah-langkah keamanan sederhana, seperti menggunakan perangkat lunak anti-virus dan mengidentifikasi potensi risiko atau penipuan dalam transaksi keuangan online mereka.

SIMPULAN

Berdasarkan hasil dan pembahasan dalam penelitian, maka dapat ditarik kesimpulan bahwa di dunia cyber banyaknya yang mempersalah gunakan internet untuk menipu orang dengan manipulasi. Di dalam cyber juga terdapat cybercrime, cybersecurity, dan cyber terrorism. Cyber terorism biasanya juga memiliki arti atau makna yang lebih kuat daripada Cybercrime, menggambarkan tindakan yang memiliki karakteristik serupa dengan serangan terorisme dunia nyata, tetapi tidak selalu.

Keamanan cyber bukan hanya tanggung jawab dari pemerintah saja, kita sebagai seseorang yang menggunkana internet dijaman sekarang juga harus menjaga data privasi kita. Untuk menjaga identitas, kita dapat melakukan beberapa tip yaitu dengan cara tidak memberikan nomor jaminan sosial kita, menghapal kata sandi atau jangan pernah menuliskan atau membawa-bawa tulisan yang ada kata sandi kita, saat menggunkan ATM pastikan tidak ada yang melihat saat kita memasukkan kata sandi, dll. Dari tips ini kita dapat meminimalisir pencurian data yang terjadi.

DAFTAR PUSTAKA

Abrori, H. (2018). Humas Sebagai Method of Commucation Dalam Membentuk Image Madrasah. *Al-Tanzim: Jurnal Manajemen Pendidikan Islam*, *2*(2), 161–166.

Anggito, A., & Setiawan, J. (2018). *Metodologi penelitian kualitatif*. CV Jejak (Jejak Publisher). https://doi.org/10.31219/osf.io/svu73

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Dermawan, A., & Akmal, A. (2020). Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi. *Journal Of Science And Social Research*, *2*(2), 39–46.

Fitri, S. N. (2022). Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, *7*(1), 104–124.

Ginting, M. H. (2018). *Tinjauan Yuridis Terhadap Pelaku Cyber Terrorism Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme*.

Herman, V. (2019). *Tinjauan Kriminologis Terhadap Kejahatan Penipuan Yang Dilakukan Melalui Media Elektronik (Studi Kasus Polda Sulsel Tahun 2016 S/D 2018)*. Universitas Hasanuddin.

Hooper, C., Martini, B., & Choo, K.-K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, *29*(2), 152–163.

Idik Saeful Bahri, S. H. (2020). *Cyber Crime Dalam Sorotan Hukum Pidana* (Vol. 159). Bahasa Rakyat.

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.

Napitupulu, D., Lubis, M. R., Revida, E., Putra, S. H., Saputra, S., Negara, E. S., & Simarmata, J. (2020). *E-Government: Implementasi, Strategi dan Inovasi*. Yayasan Kita Menulis.

Oksidelfa Yanto, S. H. (2021). *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi*. Samudra Biru.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2), 230–239.

Rohida, L. (2018). Pengaruh era revolusi industri 4.0 terhadap kompetensi sumber daya manusia. *Jurnal*

Manajemen Dan Bisnis Indonesia, *6*(1), 114–136. https://doi.org/10.31843/jmbi.v6i1.187

Sarinastiti, E. N., & Vardhani, N. K. (2017). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism New Media. *Jurnal Gama Societa*, *1*(1), 40–52.

Sidik, S. (2013). Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1–7.

Simarmata, J., Sasongko, D., Sihotang, J. I., Yuswardi, Y., Rohmah, M. F., St Amina, H. U., Arni, S., Sugianto, S., Jamaludin, J., & Akhriana, A. (2022). *Sistem Keamanan Data*. Yayasan Kita Menulis.

Simbolon, M. S. (2019). *Analisis Yuridis Terhadap Pemalsuan Identitas Kepolisian Untuk Melakukan Pencurian (Studi Polsek Medan Barat)*.

Utomo, S. (2017). Tantangan Hukum Modern Di Era Digital. *Jurnal Hukum Media Bhakti*.

Uttata, I. (2020). *Tindakan Aparatur Penegak Hukum Terhadap Pencemaran Nama Baik Melalui Media Sosial Ditinjau Menurut UU ITE Nomor 19 Tahun 2016 (Studi Kasus di Kabupaten Simeulue)*. UIN Ar-Raniry.

Yulianah, S. E. (2022). *Metodelogi Penelitian Sosial*. CV Rey Media Grafika.