 ISSN : 2549-869X

Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya

Ervina Chintia [1], Rofiqoh Nadiah [2], Humayyun Nabila Ramadhani [3], Zulfikar Fahmi Haedar [4], Adam Febriansyah [5], Nur Aini Rakhmawati S.Kom., M.Sc.Eng [6]

Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya.

[1]ervina15@mhs.is.its.ac.id
[2]rofiqoh16@mhs.is.its.ac.id
[3]humayyun16@mhs.is.its.ac.id
[4]fahmi16@mhs.is.its.ac.id
[5]febriansyah.adam16@mhs.is.its.ac.id
[6]nur.aini@is.its.ac.id

***Abstrak* - Dewasa ini Teknologi Informasi bukan lagi menjadi kata asing di telinga masyarakat Indonesia. Kebutuhan akan Teknologi Informasi menjadi semakin penting seiring perkembangan zaman yang menuntut kehadiran Teknologi Informasi di segala aspek dalam kehidupan, mulai dari ekonomi, industri hingga kesehatan. Tuntutan zaman tersebut membuat Teknologi Informasi untuk senantiasa meningkatkan keramahan bagi penggunanya. Hal ini menimbulkan pro dan kontra karena semakin ramahnya sebuah teknologi tidak hanya akan berdampak pada banyaknya pengguna, namun semakin besar pula kemungkinan pengguna untuk menggunakan Teknologi Informasi dalam perilaku kejahatan siber, istilah yang digunakan untuk kejahatan yang menggunakan Teknologi Informasi sebagai alat maupun target dari sebuah kejahatan.**
Pada *paper* ini akan dibahas mengenai kasus-kasus kejahatan siber yang paling banyak terjadi di Indonesia, apa alasan kasus tersebut bisa banyak terjadi serta bagaimana respon pemerintah dalam menangani kejahatan siber yang semakin marak terjadi di Indonesia.

Kata Kunci—Teknologi Informasi, Kejahatan Siber, Kejahatan IT, Kesadaran Privasi, Penanganan Kejahatan Siber.

I. PENDAHULUAN

Semakin berkembangnya teknologi di era yang canggih saat ini, menjadikan teknologi tidak dapat dilepaskan lagi dari kehidupan sehari-hari. Apapun kegiatan atau pekerjaan manusia saat ini telah ditopang dan bahkan sangat bergantung dengan teknologi. Salah satu yang paling berpengaruh adalah perkembangan Teknologi Informasi atau yang biasa kita sebut IT. Tanpa sadar teknologi IT ini ikut mempengaruhi budaya, sosial, dan politik pada suatu bangsa. Sehingga pada perkembangannya, selain membawa manfaat yang besar IT juga membawa dampak buruk pula. Salah satu dampak buruk yang ditimbulkan adalah adanya penyalahgunaan dari teknologi IT oleh oknum dan pihak-pihak yang tidak bertanggungjawab yang bertujuan mengambil keuntungan dengan cara-cara yang merugikan banyak orang dan bahkan melanggar hukum yang telah diatur dalam sebuah negara. Bentuk pelanggaran seperti ini kini disebut dengan "Kejahatan IT" atau yang biasa kita kenal dengan kata "IT Crime".

Kejahatan IT atau IT Crime merujuk pada kejahatan atau kegiatan ilegal yang menggunakan IT atau komputer sebagai alat atau target kejahatan. Namun istilah tersebut sebenarnya tidak awam di dunia internasional, beberapa ahli dan situs-situs teknologi terkenal menyebutnya sebagai cybercrime. Dalam bukunya, Clough(2010) mendefinisikan *cyber crime* sebagai sebuah kejahatan menggunakan media komputer atau jaringan komputer [1].

II. PEMBAHASAN

A. *Penggunaan Teknologi Informasi di Indonesia*

Indonesia merupakan salah satu negara dengan penduduk terbanyak di dunia. Dilihat dari situs Worldometers Indonesia berada di peringkat 4 dengan total 266.794.980 berada di bawah Amerika Serikat, India dan Tiongkok [2]. Didukung dengan semakin luasnya jangkauan layanan internet, serta murahnya harga perangkat pendukung penggunaan internet seperti s*martphone*, *personal computer*, tablet, laptop dan lain sebagainya membuat pengguna perangkat Teknologi Informasi tumbuh pesat di Indonesia.

Berdasarkan situs katadata.co.id, jumlah pengguna internet di Indonesia pada tahun 1998 hanya mencapai 500 ribu, sangat jauh jika dibandingkan dengan tahun 2017 yang mencapai lebih dari 100 juta pengguna. Menurut data survei APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), pengguna internet di Indonesia pada 2017 telah mencapai 142 juta jiwa atau 54,69 persen dari jumlah penduduk di Indonesia. Pengguna internet pada tahun 2016 tumbuh 7,9% dari tahun sebelumnya dan tumbuh lebih dari 600% dalam 10 tahun terakhir [3].

B. *Cybercrime*

Cybercrime merupakan kejahatan baru yang muncul sebagai akibat dari berkembangnya Teknologi Informasi. Cybercrime melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional [4]. Namun menurut penelitian lain, sarana

yang dipakai tidak hanya komputer melainkan juga teknologi [5]. Sehingga, dengan berkembangnya teknologi di Indonesia yang sangat pesat saat ini khususnya *Teknologi Informasi* menjadikan *Cybercrime* ini salah satu kasus yang harus benar-benar kita perhatikan dan kita waspadai. Karena bagaimanapun kejahatan seperti ini pasti akan terjadi dalam suatu wilayah atau negara. Tergantung bagaimana usaha suatu wilayah atau negara itu dalam menanganinya.

C. *Kasus Cybercrime di Indonesia*.

Seiring berjalannya waktu, kasus Cybercrime semakin marak terjadi di seluruh belahan dunia, begitupun Indonesia. Munculnya beberapa kasus "Cyber Crime" di Indonesia, seperti penggelapan uang di bank melalui komputer, kasus video porno yang diunggah di internet, hacker, carding atau kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet, penyebaran virus dengan sengaja di internet, *cybersquatting* yang diartikan sebagai mendaftar, menjual atau menggunakan nama domain dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain melalui internet dan kasus pencurian dokumen pemimpin negara melalui internet, semua kasus cybercrime ini menunjukkan gejala pergeseran masalah sosial dari dunia nyata. Tindak kejahatan ini dalam prateknya menggunakan teknologi telematika canggih yang sulit untuk dilihat dan dapat dilakukan di mana saja [6]. Modus dan motif cybercrime kian kompleks makadari itu tidak ada jaminan keamanan di cyberspace, dan tidak ada sistem keamanan komputer yang Para hacker akan terus mencoba untuk menaklukkan sistem keamanan yang paling canggih, dan merupakan kepuasan tersendiri bagi hacker jika dapat membobol sistem keamanan komputer orang lain [7].

Melalui situs yang dimuat oleh forbes.com, dengan judul artikelnya yaitu “The Top Cyber Security Risks In Asia-Pacific In 2017” dituliskan bahwa pada bulan Maret, varian ransomware yang dikenal sebagai KimcilWare terlihat menargetkan situs web yang menjalankan platform eCommerce Magento. Varian ini diduga telah dikembangkan di Indonesia. Selain itu juga, disebutkan bahwa para pelaku dari Asia Pasifik sangat aktif dalam kegiatan carding (perdagangan kartu kredit dengan rincian rekening bank orang lain). Taktik, teknik dan prosedur (TTPs) yang terlibat dalam carding sedang dibagikan baik dalam grup tertutup di Facebook dan di forum web yang mendalam. Peretas dari Bangladesh, Pakistan, India, Filipina dan Indonesia diamati sebagai yang paling aktif dalam hal ini [8]. Menurut survey yang dilakukan oleh salah satu aplikasi keamanan komputer yaitu Norton, yang di unggah pada *website* resminya, disebutkan bahwa dalam setahun terakhir lebih dari 978 juta orang dewasa di 20 negara cybercrime global yang berpengalaman, salah satunya Indonesia dengan total 59,45 juta orang dewasa yang menjadi pelaku cybercrime. Dan untuk kerugiannya, tidak tanggung seperti yang telah disebutkan juga oleh Norton, total kerugian konsumen yang menjadi korban cybercrime secara global, Indonesia mencapai nilai yang sangat fantastis yaitu $ 3.2 miliar [9].

Hal ini telah menjelaskan, bahwa Indonesia seharusnya lebih peduli dan paham, bahwa Cybercrime adalah kejahatan yang patut kita waspadai. Semakin sering kita terhubung dengan Internet, semakin besar pula kemungkinan kita mengalami kejahatan siber. Menurut salah satu artikel berita nasional, kasus kejahatan siber yang menonjol di Indonesia adalah ujaran kebencian. Secara umum, baik melalui media sosial maupun sarana lain, kasus ujaran kebencian yang ditangani Polri selama 2017 sebanyak 3.325 kasus. Sementara pada 2016, kasus ujaran kebencian yang ditangani Polri sebanyak 1.829 kasus [10]. Bukan hanya itu, sebenarnya masih banyak kasus siber yang terjadi di Indonesia, namun sayangnya masih belum memiliki perhatian khusus baik dari pemerintah, hingga masyarakat itu sendiri yang notabennya adalah pelaku dan juga korban kasus tersebut, yaitu Pemberitaan Berita Bohong (Hoax). Kasus Pemberitaan Berita Bohong (Hoax) adalah kasus yang paling sering terjadi, dan bahkan sering dijumpai disekitar kita, setiap hari dilakukan oleh anggota keluarga kita, teman-teman kita, oleh orang-orang disekitar kita.

D. *Penanganan Cybercrime di Indonesia*.

Dunia menghadapi dilema yang sama tentang cara memerangi cybercrime dan bagaimana cara efektif mempromosikan keamanan kepada masyarakat dan organisasi mereka. Kejahatan dunia maya, tidak seperti kejahatan tradisional yang dilakukan di satu lokasi geografis, namun dilakukan secara online dan sering tidak jelas terkait dengan lokasi geografis mana pun. Oleh karena itu, diperlukan respon global yang saling terkoordinasi terhadap masalah cybercrime [11]. Salah satunya Indonesia, kini pemerintah mempersiapkan strategi untuk menghadapi kasus Cybercrime yang mulai menjadi perhatian khusus saat ini.

Adapun upaya yang telah dilakukan pemerintah yaitu salah satunya dengan membentuk Badan Siber dan Sandi Negara (BSSN). BSSN yang dibentuk dengan mempertimbangkan bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional. Pembentukan BSSN merupakan upaya untuk menata Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber[12].

Selain itu, dalam hal ini Polri sebagai aparat penegak hukum Indonesia telah menyiapkan unit khusus untuk

menangani kejahatan cyber ini yaitu UNIT V IT/CYBERCRIME Direktorat II Ekonomi Khusus Bareskrim Polri. Polri dalam hal ini khususnya unit cybercrime menggunakan parameter berdasarkan dokumen kongres PBB tentang The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, yang merumuskan cybercrime sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain [13].

Adanya penegak, kurang sesuai jika tanpa hukum yang diberlakukan. Oleh karena itu, Indonesia pun membentuk hukum untuk mengatur Cybercrime, dalam hal ini ada 2 hukum utama yang digunakan yaitu – Hukum Telekomunikasi UU No. 36/1999 dan Hukum Information Transaction Electronics (ITE) UU No. 11/2008. Menerut pengamatan mendalam yang dilakukan oleh Leo dan Dinita terhadap sejarah kasus cybercrime di Indonesia, menunjukkan bahwa landasan hukum untuk cybersecurity masih lemah. Dibandingkan dengan negara lain, Indonesia tertinggal dalam hal kebijakan dan peraturan keamanan TIK. Misalnya di Malaysia, sudah memiliki UU Kejahatan Komputer, Digital Signature Act, Telemedicine Act (tiga dari mereka telah diberlakukan sejak 1997), Multimedia Act (1998), Payment System Act (2003) dan Personal Data Act (2010). Singapura juga memiliki satu set peraturan serupa. Kedua undang-undang yang ada memiliki keterbatasan mereka sendiri. UU Telekomunikasi, hanya mengenai lingkup telekomunikasi, namun tidak disebutkan infrastruktur telekomunikasi misalnya dalam konteks internet. Sehingga membuatnya sulit untuk menempatkan ke dalam konteks kasus-kasus tertentu. Selain itu, sementara undang-undang khusus pada cybercrime telah diberlakukan melalui Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) namun ruang lingkupnya juga terbatas, karena masih memerlukan undang-undang lain untuk melengkapi. Karena keterbatasan ini, kasus kriminal yang terkait dengan kejahatan cyber sedang terjadi dihukum dengan KUHAP Hukum Acara Pidana (UU KUHAP), Perlindungan Konsumen UU No. 8/1999, UU Hak Cipta No. 19/2002 atau UU Anti-Pornografi No.44/2008. Namun Undang-Undang Informasi dan Transaksi Elektronik No. 11/2008 terbentuk landasan pemerintahan cybersecurity terkait (serta perdebatan) negara [14].

Meskipun lemah dalam hal legislatif, Indonesia cukup kuat dalam hal teknis dan langkah prosedural. Kerja sama internasional juga tidak dianggap sebagai masalah karena Indonesia meningkatkan kerjasama internasionalnya dengan berbagai organisasi, pakar keamanan dan forum untuk meningkatkan pemahamannya terhadap ancaman global. Sebagai perwujudan dari prinsip ini dalam cybersecurity, Indonesia telah menjadi anggota penuh APCERT dan FIRST dan pendiri OIC-CERT. Adapun langkah-langkah teknis, Indonesia telah secara resmi mengakui kepatuhan persyaratan melalui SNI / ISO / EIC 27001: 2013 tentang Sistem Manajemen Keamanan Informasi. Untuk meningkatkan kesadaran keamanan dan melacak kemajuan, Indonesia memiliki kerangka tersendiri untuk menilai keamanan informasi domestic di seluruh instansi pemerintah. Indeks KAMI (Keamanan Informasi Nasional Indeks) mengevaluasi lima bidang keamanan informasi: tata kelola, manajemen risiko, kerangka kerja, manajemen aset, dan teknologi [14]. Namun, masih ada banyak pekerjaan yang diperlukan. Tidak adanya *roadmap* tata kelola nasional yang diakui secara resmi untuk keamanan siber adalah salah satu prioritas yang mendesak (ITU 2015). Sehubungan dengan penerapan standar internasional, ITU (2015) mencatat bahwa Indonesia belum secara resmi menyetujui keamanan siber nasional dan kerangka kerja. Ini juga berlaku untuk sertifikasi. Saat ini, Indonesia tidak memiliki keamanan siber nasional dan kerangka kerja yang disetujui secara resmi untuk sertifikasi dan akreditasi lembaga nasional dan professional sector umum. Asosiasi Penyedia Internet Indonesia (APJII) mengkonfirmasi temuan ini dengan menambahkan bahwa saat ini standar yang ada sebagian besar diadopsi dari entitas regional atau internasional (wawancara, 2016) [14].

E. *Kesadaran Masyarakat Terhadap Keamanan TI*

Meningkatnya Cybercrime di Indonesia telah menjadikan pemerintah dan aparat hukum melakukan beberapa antisipasi untuk menekan jumlah kejahatan diinternet melalui perubahan Undang-Undang sesuai perkembangan teknologi. Pemberian materi Etika Komputer di Perguruan Tinggi dan Pemahaman tentang kesadaran keamanan berinternet kepada para penggunanya. Namun semua kembali kepada masing-masing pengguna *Teknologi Informasi* ini untuk sadar tentang pentingnya mengamankan data-data dan aktifitasnya [15]. Namun sayangnya tingkat kepedulian pengguna dalam menjaga keamanan TI masih belum tinggi. Seperti yang telah di publikasikan pada situs Hootsuite.com diperoleh prosentasi akan sikap masyarakat Indonesia dalam merasakan peran teknologi dan perspektif mereka tentang privasinya [16].

TABEL I

PENGGUNAAN TEKNOLOGI DAN TINGKAT KEPEDULIAN TERHADAP PRIVASI

No.	Perspektif pada masalah privasi TI	Prosentasi
1.	Tingkat kepercayaan akan peluang TI dibandingkan resiko	71%
2.	Penggunaan TI dalam menyelesaikan tugas	68%
3.	Tingkat kepercayaan akan privasi data dan perlindungannya	79%

ISSN : 2549-869X

4.	Penghapusan *cookies* pada browser Internet untuk melindungi privasi	57%
5.	Penggunaan alat pemblokiran iklan untuk menghentikan iklan yang ditampilkan	50%

Selain itu peningkatan *Cybercrime* di Indonesia juga karena pengaruh kemajuan *Teknologi Informasi* itu sendiri dalam mempengaruhi budaya di Indonesia. Mulai dari (1) perbedaan pria dan wanita (2) meningkatnya rasa percaya diri (3) dan adanya tekanan [17]. Dengan budaya masyarakat di Indonesia yang telah mengakar kuat dan sangat mempengaruhi kehidupan sosialnya, kasus *Cybercrime* ini muncul dan masuk melalui celah kelemahan pada sosial budaya masyakart di Indonesia. Sehingga kesadaran masyarakat dalam kasus *Cybercrime* ini harus bisa ditanamkan lebih kuat lagi karena harus merubah budaya masyakaratnya pula.

III. ANALISA

Dengan banyaknya jenis kejahatan siber yang terjadi di Indonesia, pihak kepolisian telah melakukan perhitungan kasus-kasus kejahatan siber yang terjadi di Indonesia dengan prosentasenya masing-masing didapatlah bahwa kasus kejahatan siber yang paling banyak terjadi di Indonesia pada tahun 2017 adalah kejahatan penyebaran berita bohong atau biasa disebut berita *hoax*. Seperti yang dilansir oleh laman okezone.com, Ketua Kepolisian Republik Indonesia (atau biasa disingkat Kapolri), Jenderal Tito Karnavian mengatakan, bahwa tingkat penyebaran *hoax* yang semakin marak ini adalah dikarenakan sudah bebasnya penggunaan sosial media di kalangan masyarakat Indonesia akhir-akhir ini.

Dalam analisa kami selanjutnya, alasan mengapa kasus kejahatan siber yang paling banyak terjadi di Indonesia pada tahun 2017 dan 2018 ini adalah kasus penyebaran berita *hoax* adalah karena ditemukannya lima penyebab dari hasil studi literatur, yaitu sebagai berikut.

1. Karena bebasnya penggunaan media sosial. Kemudahan yang dijanjikan dan disajikan oleh media internet bukan hanya dimanfaatkan oleh pelaku bisnis komputer dan elektronika, namun juga mengunggah pelaku bisnis yang bergerak di bidang penerbitan dan pemberitaan [18]. Akibat pertumbuhan dari perkembangan internet yang cukup signifikan dari tahun ke tahun tersebut menyebabkan semakin maraknya penyebaran berita bohong atau *hoax*. Dalam menyebarkan berita *hoax*, biasanya pihak-pihak yang tidak bertanggungjawab itu melakukan suatu kebohongan dan menyebarkan informasi yang tidak benar secara sadar. Hal itu sama sekali tidak menimbulkan kekhawatiran bagi para pelaku dalam melakukan aksinya dikarenakan kurnagnya penyaringan berita di media social sehingga berita apapun yang dibagikan dapat dengan mudah tersebar [17].

   Di sisi lain, hal lain yang dapat mendorong mudahnya berita *hoax* tersebut tersebar secara cepat adalah dari sisi masyarakat Indonesia sendiri. Masyarakat masih belum memiliki pemahaman dan pengetahuan hukum yang memadai tentang dampak dan ancaman dari penyebaran berita bohong atau hoax. Selain itu, mudahnya penyebaran berita *hoax* tersebut yang dilakukan oleh masyarakat ke berbagai media social dapat menyebabkan penyebaran berita tersebut menjadi massif, sehingga akan susah untuk dilakukan klarifikasi [18]. Didapat pada Tabel 1, terlihat pada poin 3 bahwasanya tingkat kepercayaan akan privasi data dan perlindungannya oleh masyarakat mencapai 79%, dimana hal itu menunjukkan bahwa sebagian besar masyarakat Indonesia merasa bahwa data-data mereka sudah cukup aman. Dari sini dapat diketahui bahwa untuk mencegah terjadinya penyebaran berita *hoax* pada poin satu ini adalah dengan memberikan edukasi mengenai UU ITE dan sosialisasi mengenai bahaya penyebaran berita tanpa dikethaui sumbernya dengan jelas kepada masyarakat.
2. Karena merupakan kejahatan yang terlihat sehingga mudah diadukan. Kasus kejahatan penyebaran berita bohong yang dilakukan melalui media social ini merupakan suatu kejahatan yang dapat dengan mudah diketahui dan dilacak kebenarannya. Setiap kali terdapat berita yang terindikasi tidak benar, maka si penerima berita dapat dengan langsung melaporkan kepada pihak berwajib. Dengan mudahnya deteksi kebenaran dan pelaporan ini menyebabkan kasus penyebaran berita *hoax* dapat terhitung dengan baik jumlahnya oleh pihak kepolisian.
3. Karena kurangnya pemahaman mengenai UU ITE oleh kepolisian Indonesia. Mudahnya pelaporan oleh masyarakat terhadap suatu kasus tidak sebanding dengan mudahnya penanganan dan penindakan oleh pihak kepolisian. Sumber daya manusia di instansi kepolisian saat ini masih banyak yang terbatas dalamn hal penguasaan ITE (UU No. 19 Tahun 2016 Tentang ITE Pasal 28) [17]. Semua hukum dan undang-undang yang telah dibuat oleh pihak negara, apabila kurang dipahami oleh pihak yang bertanggungjawab, maka pembuatan undang-undang tersebut akan percuma. Hal ini sangat disayangkan, dimana kunci dari keberhasilan dalam penegakan hukum, yaitu penegak hukum itu sendiri, ternyata kurang begitu memahami bagaimana cara penangangan kasus penyebaran berita *hoax*, sehingga menyebabkan kasus semacam ini banyak yang dibiarkan saja dan pelaku bebas melakukan tindakannya lagi. Namun, untuk mengantisipasi terjadinya pemberitaan

ISSN : 2549-869X

hoax tersebut, kini pihak kepolisian telah menyiapkan beberapa tindakan, yaitu penyimpanan regulasi, melakukan klarifikasi, memberikan serangan balik dan melakukan investigasi.

4. Karena dalam UU dinyatakan bahwa kasus penyebarang berita *hoax* hanya dapat diperdanakan apabila terdapat pihak yag dirugikan, sehingga membuat para pelaku penyebar *hoax* yang tidak begitu memberi dampak negative yang signifikan tidak dapat ditindak lanjuti dan menyebabkan ia menjadi mampu melakukan tindakan kejahatannya lagi.
5. Karena kepolisian Indonesia lebih berfokus pada penyelesaian kasus lain (pencemaran nama baik) daripada kasus penyebaran *hoax* untuk segera ditangani.

Seperti yang dilansir oleh laman berita bbc.com, kasus pencemaran nama baik dan ujaran kebencian menjadi bentuk kasus kejahatan siber terbanyak yang ditangani oleh kepolisian. Hampir 45% dari total kejahatan siber yang terjadi di Indonesia merupakan kejahatan pencemaran nama baik dan ditangani dengan segera oleh pihak kepolisian. Hal ini menyebabkan kasus-kasus kejahatan siber lain yang lebih merugikan, atau kasus penyebaran berita *hoax* ini. Maka dengan terjadinya alasan seperti ini, hal ini dapat menyebabkan kasus penyebaran berita *hoax* tidak segera ditangani oleh pihak kepolisian, sehingga menyebabkan para pelakunya bebas mengulangi kejahatannya kembali.

IV. KESIMPULAN

Kejahatan siber sejatinya adalah suatu kejahatan yang menggunakan alat komputer dan teknologi sebagai media kejahatannya, dimana terdapat tiga pihak yang terlibat langsung dalam terjadinya kasus tersebut, yaitu pihak kepolisian sebagai aparat penegak hukum, pihak masyarakat umum sebagai korban, dan pihak pelaku. Demi untuk mencegah atau menangani terjadinya kasus kejahatan siber (yang notabene cukup membahayakan daripada kejahatan non siber), diperlukan keterlibatan pihak kepolisian dan masyarakat. Kedua pihak ini diperlukan untuk sama-sama menjadi lebih pintar dan paham mengenai undang-undang atau bahaya dari suatu kejahatan tersebut daripada si pelaku agar kasus kejahatan-kejahatan siber tidak dapat dilakukan dengan lancar oleh pelaku kejahatan.

Untuk kejahatan siber yang paling sering terjadi di Indonesia, yaitu penyebaran berita *hoax*, diperlukan adanya pemahaman kuat terhadap dampak apa yang sekiranya akan terjadi dari kejahatan tersebut, juga terhadap undang-undang yang telah mengaturnya, agar didapatkan suatu formula khusus untuk dapat mencegah terjadinya kasus penyebaran berita *hoax* kembali.

REFERENSI

[1] J. Clough, *Principles of cybercrime, second edition*. 2015.
[2] Worldometers.info, “Countries in the World by population,” 2016.
[3] Databooks.co.id, “Berapa jumlah pengguna internet Indonesia,” 2018. [Online]. Available: https://databoks.katadata.co.id/datapublish/2018/02/20/berapa-jumlah-pengguna-internet-di-indonesia.
[4] D. A. Arifah, “Kasus Cybercrime Di Indonesia,” *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.
[5] D. A. N. Dustri, D. A. N. Aspek, and H. Yang, “Mengenal dan Mengantasipasi Kegiatan Cybercrime pada Aktifitas Online Sehari-hari dalam Pendidikan, Pemerintahan, dan Industri dan Aspek Hukum Yang Berlaku.,” *Snikom*, 2014.
[6] R. Anto, “Kasus-Kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Kasus-Kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Komunikasi yang Meresahkan Masyarakat,” no. July, pp. 0–12, 2018.
[7] I. Ali, “Kejahatan Terhadap Informasi (Cybercrime) dalam Konteks Perpustakaan Digital,” vol. V, no. 1, 2012.
[8] F. Sidek and J. Rubbi-clarke, “The Top Cyber Security Risks In Asia-Paci c In 2017,” *www.forbes.com*, pp. 1–8, 2018.
[9] Symantec Corporation, “2017 Norton Cyber Security Insights Report - Global Results,” 2017.
[10] A. N. K. Movanita, “Ini Hasil Kerja Polri Perangi Kejahatan Siber Sepanjang 2017 - Kompas.com,” *Kompas.com*, pp. 1–5, 2017.
[11] H. Jahankhani, A. Al-Nemrat, and A. Hosseinian-Far, “Cybercrime classification and characteristics,” *Cyber Crime Cyber Terror. Investig. Handb.*, no. November, pp. 149–164, 2014.
[12] A. Budiman, “Optimalisasi Peran Badan Siber dan Sandi Nasional,” vol. IX, no. 12, 2017.
[13] P. R. Golose, “Perkembangan Cybercrime Dan Upaya Penanganannya Di Indonesia Oleh Polri,” vol. 4, 2006.
[14] L. K. Nugraha and D. A. Putri, “Mapping the Cyber Policy Landscape: Indonesia,” no. November, 2016.
[15] M. Danuri, “Trend cyber crime dan teknologi informasi di indonesia,” no. January, 2018.
[16] S. Kemp, “Digital in 2018 in Southeast Asia,” 2018.
[17] M. R. Marwan and Ahyad, “Analisis Penyebaran Berita HOAX di Indonesia.”
[18] M. Elvia and D. R. Monica, “Peran Kepolisian dalam Penanggulangan Tindak Pidana Penyebar Berita Bohong (Hoax),” 2018.