JURNAL ILMIAH DINAMIKA SOSIAL

VOLUME 4 NOMOR 1 2020 | E-ISSN : 2581-2424 | P-ISSN : 2597-3657 | Website : journal.undiknas.ac.id

PENINGKATAN RASIO KEJAHATAN *CYBER* DENGAN POLA INTERAKSI *SOSIO ENGINEERING* PADA PERIODE AKHIR ERA *SOCIETY 4.0* DI INDONESIA

Sandryones Palinggi[1], Srivan Palelleng[2], Lutma Ranta Allolinggi[3]

1) Institut Teknologi Bandung; 2)3) Universitas Kristen Indonesia Toraja
23217112@std.stei.itb.ac.id

Received: 29 December 2019 | Reviewed: 3 January 2020 | Accepted: 2 February 2020

ABSTRAK

Lompatan evolusi teknologi ditandai dengan munculnya beragam teknologi baru khususnya di bidang ICT seperti Fifth Generation, High Throughput Satellite, High Altitude Platform Station, Artificial Intelegent, Blockchain dan Big Data, memberikan pengaruh terhadap pola interaksi antar manusia, semenjak era internet telah menjadi bagian penting dalam struktur kebutuhan masyarakat. Peran dari internet telah menggeser tatanan interaksi manusia secara umum namun memiliki manfaat besar dalam sistem peradaban masyarakat Society 4.0. Dengan adanya kemajuan teknologi, secara tidak langsung memberikan gambaran bahwa era Society 4.0 akan segera berakhir, digantikan dengan era Society 5.0. Diakhir era Society 4.0 dimana telah terintegrasi dengan internet, kejahatan cyber telah ikut berevolusi dengan menggunakan pola pendekatan interaksi sosio engineering yang berpotensi merugikan banyak pihak. Society 5.0 adalah era teknologi modern dengan mengandalkan manusia sebagai komponen utamanya. Metoda penelitian yang digunakan dalam penelitian ini adalah deskriptif kualitatif dengan pendekatan studi literatur dengan mengumpulkan informasi secara aktual dan terperinci, mengidentifikasi masalah, membuat perbandingan atau evaluasi. Hasil dan kesimpulan dari penelitian ini adalah peningkatan kesadaran masyarakat Indonesia dalam menghadapi era Society 5.0 dan tetap waspada terhadap bentuk-bentuk perubahan kejahatan cyber seperti penipuan dan pencurian data maupun informasi penting yang dimiliki

Kata Kunci : Kejahatan *Cyber*, *Sosio Engineering*, Teknologi, *Society 4.0*

Korespondensi:
Institut Teknologi Bandung
Jl. Ganesha No.10, Lb. Siliwangi
Kota Bandung, Jawa Barat
E-mail: 23217112@std.stei.itb.ac.id

ABSTRACT

The leap in technological evolution is marked by the emergence of a variety of new technologies, especially in the field of ICT such as Fifth Generation, High Throughput Satellite, High Altitude Platform Station, Artificial Intelligence, Blockchain and Big Data, giving an influence on patterns of interaction between humans, since the internet era has become an important part in community needs structure. The role of the internet has shifted the order of human interaction in general but has great benefits in the civilization system of Society 4.0. With the advances in technology, it indirectly provides a picture that the era of Society 4.0 will soon end, replaced with the era of Society 5.0. At the end of the era of Society 4.0, which has been integrated with the internet, cyber crime has also evolved by using a socio-engineering interaction approach pattern that has the potential to harm many parties. Society 5.0 is the era of modern technology by relying on humans as its main component. The research method used in this research is descriptive qualitative approach to the study of literature by gathering actual and detailed information, identifying problems, making comparisons or evaluations. The results and conclusions of this research are increasing the awareness of the Indonesian people in facing the era of Society 5.0 and remain vigilant of the changing forms of cyber crime such as fraud and theft of data and important information held

Keywords: *Cyber Crimes, Social Engineering, Technology, Society 4.0*

PENDAHULUAN

Pola interaksi antar sesama manusia telah banyak mengalami pergeseran secara signifikan. Banyaknya variabel pendukung telah menjadikan manusia sebagai subjek yang terus menerus selalu mengalami perubahan pola interaksi. Zaman modern seperti saat ini, interaksi yang terjalin tidak hanya dalam dunia nyata, tetapi juga meliputi pola interaksi dalam dunia maya. Secara tanpa disadari, perubahan demi perubahan telah mengubah banyak paradigma sosial dalam masyarakat dunia khususnya di Indonesia. (Ariansyah, 2015; Fauzi, Harly, & Hs, 2012; Wardiana, 1994). Era baru yang dikenal dengan sebutan *digitalization era* telah merubah banyak hal dalam seni berkomunikasi dan interaksi sosial kemasyarakatan. Hadirnya platform berupa aplikasi *chatting* berbasis IP (*Internet Protocol*) telah menggerus pola interaksi secara langsung antar manusia. Selain itu, platform *chatting* dari media sosial, telah mengantarkan manusia ke tingkat yang lebih mengutamakan literasi tulisan daripada literasi bahasa langsung. (Ariansyah, 2015; Fauzi et al., 2012; Wardiana, 1994)

Modernisasi dan interaksi percakapan menggunakan platform *chatting* berbasis IP, didahului oleh pola interaksi percakapan menggunakan SMS (*Short Message Service*) atau layanan pesan singkat. Dalam dunia telekomunikasi khususnya seluler, SMS menandai

generasi teknologi ke-2 atau dikenal dengan sebutan 2G (*Second Generation*). Kendati tidak sepopuler dulu, pola interaksi menggunakan SMS masih cukup sering digunakan sebagai alternatif terakhir dalam pola interaksi yang mengandalkan teknologi pesan singkat dalam bertukar informasi kepada orang lain terlebih untuk daerah-daerah di pelosok (*rural*) yang masih mengandalkan layanan 2G dalam komunikasi dan interaksi. (Ariansyah, 2015; Fauzi et al., 2012; Wardiana, 1994). Perubahan besar-besaran dialami oleh pengguna seluler, ditandai dengan semakin populernya platform *chatting* berbasis IP yang dimulai sejak era BBM (*Blackberry Messager*). Hingga saat ini platform *chatting* yang paling populer adalah *WhatsApp*, menyebabkan SMS telah beralih peran secara signifikan. Saat ini, SMS hanya digunakan sebagai media menyampaikan informasi satu arah yang dikenal dengan istilah *Broadcast*. Provider layanan komunikasi seluler memilih tetap menggunakan media SMS dikarenakan jauh lebih efektif dibandingkan ketika menggunakan platform berbasis IP disamping pertimbangan bahwa tidak seluruh wilayah di Indonesia, terlebih untuk daerah *rural*, tersentuh dengan kemajuan teknologi seluler seperti 4G (*Fourth Generation*).

Kecenderungan akan perubahan pola interaksi seperti yang dilakukan oleh penyedia jasa seluler, sedikit banyak memberikan ruang terhadap munculnya jenis kejahatan baru dari para pelaku kejahatan untuk mengambil keuntungan dari ketidaktahuan, dan ketidakpedulian masyarakat terhadap kejahatan *cyber*. Sering kali didapati SMS yang masuk ke telepon seluler merupakan bentuk informasi palsu tentang penipuan yang berkedok hadiah undian dari perusahaan besar maupun dari BUMN. Dari keseluruhan kasus yang terkait dengan kejahatan *cyber*, kasus penipuan berbasis online memiliki rasio tertinggi mencapai 1243 kasus dari Januari hingga Juli 2019. Para korban tidak menyadari bahwa pola interaksi dari para pelaku kejahatan menggunakan metode pendekatan *sosio engineering* dalam menarik minat calon korban. Korbannya pun beragam, dari kalangan berpendidikan tinggi sampai yang tidak berpendidikan, dari usia tua hingga usia remaja, bahkan dari kalangan profesional dan ICT (*Information and Communication of Technology*) yang notabenenya sangat akrab dengan jenis pola-pola kejahatan *cyber* telah banyak menjadi korban kejahatan dengan metode pendekatan *sosio engineering* seperti yang dialami oleh Roy Suryo, seorang pakar ICT Indonesia. (Detikinet, 2014)

Jika dikaitkan dengan fenomena di era digitalizasi dan penggunaan internet secara massif yang dikenal dengan era *Society 4.0*, perubahan pola interaksi seperti kejahatan *cyber* meliputi penipuan dan semacamnya, seharusnya mampu ditanggulangi oleh masing-masing

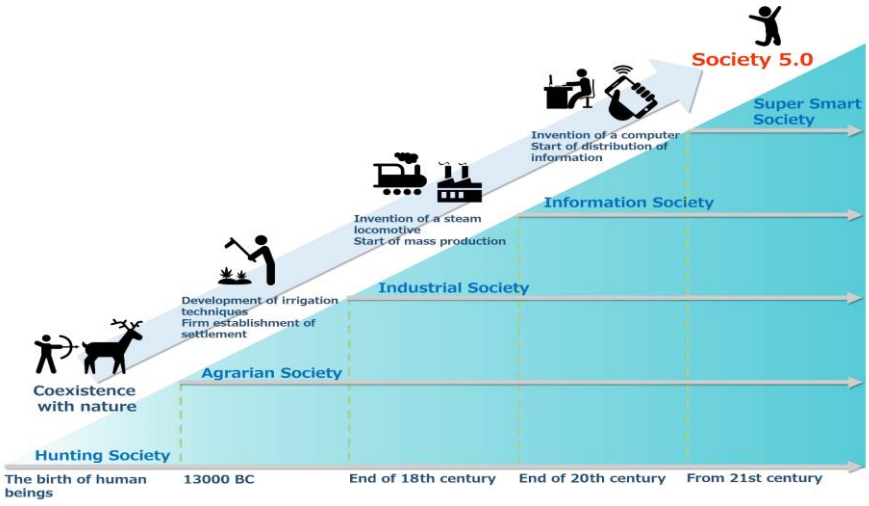
individu modern, namun kenyataannya tidaklah demikian. Banyak faktor-faktor pendukung mengapa kejahatan *cyber* masih saja menjadi sesuatu menakutkan dan dapat memberikan dampak kerugian yang luar biasa bagi korbannya. (Government of Japan, 2018; Keidanren, 2016) Tujuan dari penelitian ini adalah memberikan gambaran deskriptif yang disertai dengan contoh kasus kejahatan dengan pola yang sangat rapi terkait kejahatan *cyber*. Selain itu, penelitian inipun memberikan penjelasan mengenai interaksi secara sosial dengan menggunakan metode pendekatan *sosio engineering* sehingga mampu diantisipasi secara lebih baik di akhir era *Society 4.0*. Pola interaksi yang diciptakan oleh para pelaku kejahatan merupakan sebuah algoritma yang dapat dipecahkan dangan kesiapan tiap-tiap individu untuk menganalisa pola pendekatan secara lebih tajam terkait kejahatan *cyber* khususnya jenis kejahatan berupa penipuan. Penulis merasa bahwa sudut pandang dari ICT terkait peningkatan kejahatan *cyber* dengan menggunakan pola interaksi *sosio engineering* layak diangkat dalam sebuah kajian penelitian sebagai bentuk kepedulian terhadap maraknya kasus yang terjadi khususnya di akhir era *Society 4.0* menuju era *Society 5.0*.

KAJIAN TEORI

Lompatan Evolusi Teknologi pada Periode Akhir era *Society 4.0*

Awal tahun 2019, negara Jepang memperkenalkan sebuah konsep baru yang dikenal dengan istilah *Society 5.0*, dimana konsep dan tujuannya dipersiapkan untuk menggantikan era *Society 4.0* yang saat ini berada di penghujung periode. Konsep *Society 5.0* dipakai sebagai solusi dari kemajuan *Revolusi Industri 4.0* yang mana dikhawatirkan akan menggerus peranan dari manusia khususnya dalam kehidupan bermasyarakat. Kemajuan teknologi yang saat ini dikembangkan secara kontinyu dan menghabiskan banyak investasi, telah memberikan rasa khawatir akan terjadinya disintegrasi antar manusia dan perangkat cerdas. (Government of Japan, 2018; I-Scoop, 2017; Keidanren, 2016; Prima, 2019). *Society* sendiri telah mengalami banyak perubahan evolusi dalam perjalanan interaksi manusia. Dikutip dari I-Scoop dengan judul *From Industry 4.0 to Society 5.0: the Big Societal Transformation Plan of Japan* (I-Scoop, 2017), disebutkan bahwa evolusi *Society* telah ada sejak zaman dahulu. *Society 1.0* adalah zaman dimana manusia berada pada era berburu dan periode awal mengenal tulisan. *Society 2.0* adalah periode dimana manusia sudah mulai melakukan aktivitas secara bersama seperti bercocok tanam dan aktivitas dalam mengelola tanah sebagai pengganti era berburu.

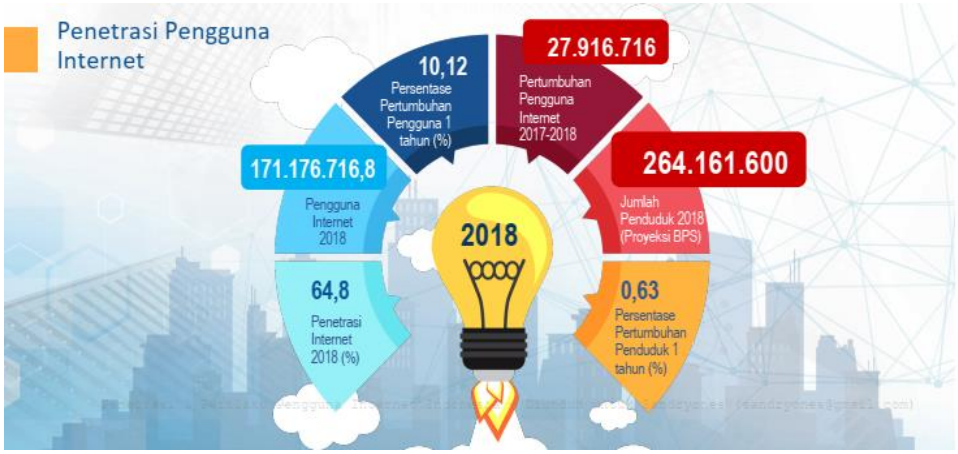
Society 3.0 dimana manusia sudah menggunakan mesin sebagai sebuah penunjang kehidupan dan membantu manusia untuk melakukan segala aktifitias khususnya dalam bekerja. Periode ini pula dikenal dengan sebutan era *Revolusi Industri 1.0* yang dimulai di tanah Britania pada tahun 1784. *Society 4.0* merupakan periode yang dialami manusia saat ini, dimana penggunaan perangkat elektronik telah dipakai secara aktif seperti komputer untuk membantu menyelesaikan pekerjaan manusia yang bersifat kompleks dan rumit. Periode *Society 4.0* lahir bersamaan dengan periode *Revolusi Industri 3.0*, dimana penemuan perangkat elektronik dan perangkat komputer mulai dikembangkan pada tahun 1969. Sedangkan era *Society 5.0*, yang diperkirakan akan lahir bertepatan dengan era *Revolusi Industri 4.0* dimana teknologi maju telah menguasai seluruh aspek kehidupan baik secara individu maupun secara berkelompok. Saat ini, baik periode *Society 4.0* maupun era *Revolusi Industri 3.0*, sama-sama berada pada masa periode akhir.



Gambar 1. Evolusi Perkembangan *Society* di Dunia (Keidanren, 2016)

Lompatan evolusi teknologi dalam 50 tahun terakhir ini, sedikit banyak telah berpengaruh terhadap pola interaksi antar manusia, terlebih semenjak era internet telah menjadi bagian penting dalam struktur kebutuhan masyarakat khususnya di Indonesia sejak tahun 2000. Evolusi seluler yang dimulai sejak masuknya Generasi ke-3 yang disebut dengan 3G (*Third Generation*), telah membawa perubahan yang signifikan dalam kehidupan masyarakat Indonesia. Kemajuan teknologi seluler mengalami periode perubahan secara massif sejak perangkat seluler *Blackberry* diperkenalkan di Indonesia pada pertengahan Desember 2004 dan benar-benar *booming* pada tahun 2010, secara tanpa disadari meningkatkan kebutuhan akan

akses internet yang secara eksponensial terus meningkat dari hari ke hari. (Qomariastuti, 2009). Berdasarkan pada Laporan Tahunan yang dikeluarkan oleh Asosiasi Penyedia Jasa Internet Indonesia pada tahun 2018 dengan judul Penetrasi dan Profil Pengguna Internet di Indonesia (APJII, 2018), disebutkan bahwa tingkat penetrasi pengguna internet mencapai 171,176 juta orang dari total populasi Indonesia yang berkisar sekitar 264,161 juta penduduk. Ini berarti bahwa sekitar 64,8% merupakan pengguna aktif internet di Indonesia sedangkan 35,2% bukan merupakan pengguna aktif internet.



Gambar 2. Penetrasi Pengguna Internet di Indonesia (APJII, 2018)

Penelitian terkait evolusi seluler khususnya Generasi ke-5 yang dikenal dengan sebutan 5G (*Fifth Generation*), turut mendorong perubahan besar-besaran dalam struktur teknologi digital guna menyokong kehidupan masa depan. Dengan *througput* yang mencapai 100 kali lebih tinggi dibandingkan dengan teknologi 4G (*Fourth Generation*), memungkinkan perangkat cerdas dapat terintegrasi dengan sangat baik dikemudian hari. Tidak hanya itu, kemajuan di bidang satelit pun begitu pesat dengan munculnya teknologi satelit dengan kecepatan tinggi menggunakan multi *spot beam* yang dikenal dengan istilah *High Throughput Satellite* (HTS) dan semakin memperkaya konektivitas antar teknologi. Teknologi HTS merupakan evolusi dari teknologi satelit konvensional dimana salah satu bentuk evolusinya adalah penggunaan satu antena dengan *aperture* 17,5 derajat menjadi banyak antena dengan *aperture* 0,2 – 0,5 derajat.

Selain kemunculan 2 teknologi baru di bidang seluler dan *space segment* yaitu satelit, teknologi *High Altitude Station Platform* (HAPS) juga sedang dalam pengembangan demi mendukung program *Indonesia Broadband Plan* (Kominfo, 2016). Proyek Palapa Ring (*Palapa Ring Optical Cable Project* — PPP) yang menghubungkan seluruh daerah di Indonesia dalam rangka peningkatan literasi digital menggunakan Fiber Optik Bawah Laut menjadi pelengkap integrasi masa depan teknologi Indonesia khususnya dalam membangun infrastruktur bidang telekomunikasi. Peningkatan secara massif ini dapat membawa Indonesia menjadi negara maju dengan berbasis pada teknologi digital. Dalam skala global, perubahan dan perkembangan teknologi terus meningkat. Ditemukannya teknologi seperti *Artificial Intelegent* dalam mendukung integrasi manusia dan semua perangkat robotik, *Blockchain* yang terkait dengan digital perbankan, bahkan *Big Data* yang kelak menjadi kontrol dalam jalur lalu lintas data trafik masa depan. Semua perkembangan teknologi akan bermuara pada satu tujuan yaitu mempermudah dan mengefisienkan kerja dari manusia. Dengan adanya kemajuan-kemajuan teknologi yang disebutkan di atas, maka secara tidak langsung memberikan persepsi bahwa era *Society 4.0* akan segera berakhir dan digantikan oleh sebuah perubahan yaitu era *Society 5.0* dimana periode baru ini akan mengubah pola interaksi manusia secara signifikan.

Definisi *Sosio Engineering*

Pada kenyataannya *sosio engineering* dapat didefinikan tergantung pada keadaan itu mengelilingi serangan itu. *Sosio Engineering* sebenarnya adalah kecenderungan manipulasi menggunakan tingkat kepercayaan untuk mendapatkan informasi sensitif yang diperlukan demi mendapatkan suatu akses ke dalam sistem. *Sosio Engineering* tidak memerlukan keahlian teknis tingkat tinggi tetapi membutuhkan *skill* individu. (Dinesh, 2014). *Sosio engineering* pada prinsipnya berupaya mengubah masyarakat ke arah yang dikehendaki. Dengan kata lain, *sosio engineering* merupakan perubahan sosial yang direncanakan (*planned social change*). Dalam *sosio engineering* diupayakan kiat-kiat dan strategi-strategi untuk menjadikan kehidupan sosial menjadi lebih baik. *Sosio engineering* dilakukan karena situasi sosial berjalan tidak sesuai dengan apa yang diharapkan, perubahan sosial akibat modernisasi lebih banyak menimbulkan masalah-masalah sosial. (Saleh & Arif, 2018). Pengertian *sosio engineering* dalam artian lain dapat didefinisikan sebagai suatu teknik memperoleh data / informasi rahasia dengan cara mengeksploitasi kelemahan manusia. Banyak metode yang digunakan pelaku kejahatan dalam melancarkan usahanya agar bisa mendapatkan apa yang diinginkan.

Biasanya dilakukan dengan cara memanfaatkan sisi psikologis seperti bersikap ramah, memuji, ataupun melakukan suatu hal yang berlebihan agar lebih dekat dengan calon korban seperti dengan cara membujuk. Selain itu, sasaran utama dari *sosio engineering* adalah untuk memperoleh akses illegal ke dalam suatu sistem atau informasi ke dalam sebuah sistem dengan melakukan *fraud* (penipuan atau kecurangan), penyusupan ke dalam jaringan, aktivitas mata-mata, pencurian identitas, dan menghadirkan gangguan pada sistem atau jaringan. (Junaedi, 2017). Dalam konteks *sosio engineering*, hakikat dari manusia adalah memiliki tenggang rasa, dan sifat gotong royong. Tidak ada yang salah dari hakikat sifat dasar tersebut. Namun, inipulah yang menjadi celah dalam penerapan metode *sosio engineering* yang begitu terasa dari sudut pandang aspek sosial kebudayaan. Dari aspek pengetahuan, memegang kunci penting berhasil tidaknya pendekatan *sosio engineering* diterapkan. Para pelaku *sosio engineering* cenderung mendekati calon korban yang memiliki tingkat pengetahuan atau latar pendidikan yang rendah yang kemudian dapat membangkitkan kepercayaan antar relasi. (Pilliang, 2012; Suherman, Widodo, & Gunawan, 2017)

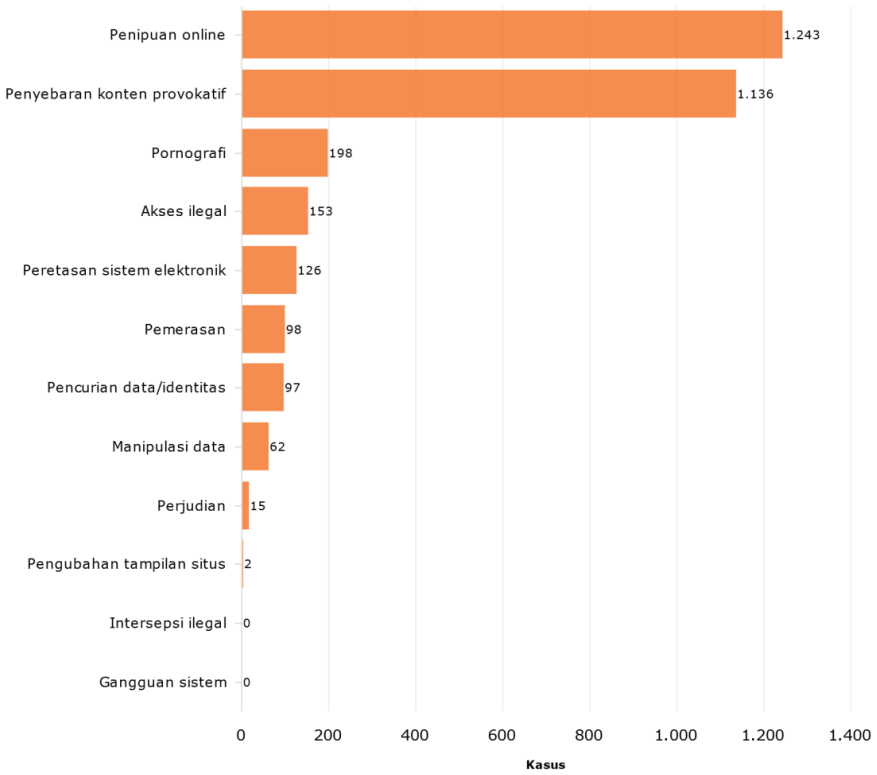
METODE PENELITIAN

Metode penelitian yang digunakan dalam penulisan artikel ini adalah deskriptif kualitatif.Adapun penelitian deskriptif kualitatif ditujukan untuk mengumpulkan informasi secara aktual dan terperinci, mengidentifikasi masalah, membuat perbandingan atau evaluasi, dan menentukan apa yang dilakukan orang lain dalam menghadapi masalah yang sama dan belajar dari pengalaman mereka untuk menetapkan rencana dan keputusan di waktu mendatang. Dengan demikian, penelitian deskriptif kualitatif hanyalah menguraikan tanggapan terhadap situasi atau peristiwa, sehingga tidak menjelaskan hubungan kausalitas maupun melakukan uji hipotesis. Menurut Burhan Bungin, metode literatur adalah salah satu metode pengumpulan data yang digunakan dalam metode penelitian sosial untuk melacak data catatan peristiwa (Bungin, 2011). Selanjutnya, literatur yang digunakan oleh penulis untuk mengumpulkan data termasuk sumber-sumber dari penelitian sebelumnya, seperti jurnal, buku referensi, observasi dan dokumentasi online yang terkait pengembangan dari kejahatan dunia maya. Analisis seperti ini merupakan teknik analisis yang dilakukan dengan menarik kesimpulan dengan melakukan identifikasi karakteristik khusus atas suatu pesan secara objektif dan sistematik.

PEMBAHASAN

Statistik Kejahatan *Cyber* di Indonesia pada *Quartal*-1 hingga *Quartal*-3 Tahun 2019

Apabila dilihat secara jumlah pengguna aktif internet khususnya di Indonesia pada tahun 2018 yang mencapai 64,8% atau 171,176 juta dimana terjadi peningkatan pengguna sebesar 27,916 juta orang dari tahun sebelumnya, maka tidak mengherankan apabila berbagai kasus kejahatan *cyber* ikut berevolusi mengikuti perkembangan teknologi yang ada. Keamanan data pribadi saat ini begitu beresiko untuk diambil alih oleh pihak-pihak yang tidak bertanggung jawab dan berpotensi sangat merugikan. (APJII, 2018). Dikutip dari situs Katadata dengan judul Penipuan Online, Kejahatan Siber yang Paling Banyak Dilaporkan, yang diterbitkan pada Oktober 2019 (Lidwina & Fitra, 2019), disebutkan bahwa jumlah laporan perihal penipuan secara online paling mendominasi, yakni sebanyak 1.243 kasus untuk periode Januari 2019 sampai Juli 2019 diantara seluruh laporan kejahatan *cyber* yang berjumlah 3.130 kasus terlapor di Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri.



Gambar 3. Jumlah Laporan Kasus Kejahatan *Cyber* pada *Quartal*-1 hingga *Quartal*-3 Tahun 2019 (Lidwina & Fitra, 2019)

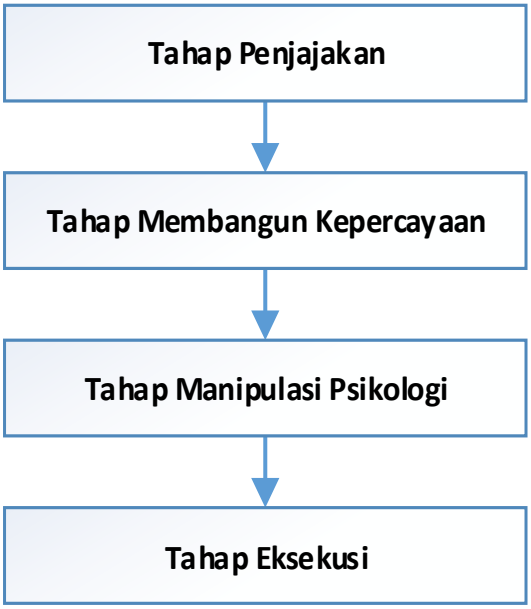
Berdasarkan pada Gambar 3 di atas, kasus kejahatan *cyber* berupa penipuan online berada pada peringkat pertama dengan jumlah kasus terlapor sebanyak 1.243 jumlah kasus, diikuti dengan kasus penyebaran konten provokatif sebanyak 1.136 jumlah kasus. Kemudian berturut-turut diikuti dengan kasus pornografi sebanyak 198 jumlah kasus, akses ilegal sebanyak 153 jumlah kasus, peretasan sistem elektronik sebanyak 126 jumlah kasus, pemerasan sebanyak 98 jumlah kasus, pencurian data / identitas sebanyak 97 jumlah kasus, manupulasi data sebanyak 62 jumlah kasus, perjudian 15 jumlah kasus, dan perubahan tampilan situs sebanyak 2 jumlah kasus, pada periode Januari 2019 hingga Juli 2019.

Dikutip dari situs Republika dengan judul Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber, yang diterbitkan pada April 2015 (Suciati Saputri & Indrawan, 2015), disebutkan bahwa tingkat kejahatan *cyber* di Indonesia menempati peringkat ke-2 di dunia setelah Ukraina. Menurut Rudiantara, Menteri Komunikasi dan Informatika Republik Indonesia periode 2014 – 2019, kasus kejahatan tersebut paling banyak adalah terkait peretasan terlebih di sektor perbankan. Hal ini disebabkan oleh tingkat standar keamanan internasional yang berbeda di tiap-tiap negara. Dengan peningkatan kejahatan *cyber* di Indonesia, pemerintah Republik Indonesia membentuk sebuah organisasi pemerintah yang memiliki tugas untuk melaksanakan keamanan *cyber* secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan *cyber* bernama Badan Siber dan Sandi Negara (BSSN) di tahun 2017 melalui Peraturan Presiden (Perpres) Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara yang selanjutnya disempurnakan melalui Perpres Nomor 133 tahun 2017 tentang Perubahan atas Perpres Nomor 53 tahun 2017 pada tanggal 16 Desember 2017 dan bertanggung jawab langsung kepada Presiden (BSSN, 2018).

Kejahatan *Cyber* dengan Metode Pendekatan *Sosio Engineering*

Beberapa pendapat mendefinisikan *sosio engineering* sebagai upaya untuk melakukan manipulasi terhadap data maupun informasi dengan menggunakan pendekatan secara psikologis terhadap calon korban. Metode pendekatan *sosio engineering* paling umum ditemukan dalam kasus penipuan secara online yaitu melakukan kontak langsung kepada calon korban, baik berupa telepon *direct* maupun melalui komunikasi media *chatting* yang terintegrasi dengan layanan berbasis IP ataupun via SMS. Dikutip dari jurnal dengan judul *Social Engineering : The Human Factor* (Dinesh, 2014), disebutkan bahwa pengertian dari *sosio engineering* adalah praktek menipu seseorang, baik secara langsung, melalui telepon,

atau menggunakan komputer, dengan tujuan jelas melanggar beberapa tingkat keamanan, baik secara pribadi maupun secara profesional dalam dunia pekerjaan. Dalam jurnal tersebut juga disebutkan alur tahapan utama dalam metode pendekatan *sosio engineering* seperti yang diperlihatkan pada Gambar 4.



Gambar 4. Alur Tahapan Utama dalam *Sosio Engineering* (Dinesh, 2014)

Dari Gambar 4 dapat diurai secara keseluruhan proses tahap demi tahap sebagai bagian dari alur utama sebuah rekayasa sosial. Tahap Penjajakan (*Footprinting*) adalah tahap dimana proses pengumpulan data terkait informasi mengenai target, calon korban serta lingkungan sekitar demi meningkatkan peluang keberhasilan. Dalam kasus yang sering dijumpai di Indonesia yakni penipuan berkedok hadiah undian, dimana pelaku kejahatan menelpon secara random nomor kontak seluler. Kontak seluler ini cenderung didapatkan dari akun media sosial yang terdaftar. Dari proses ini jelas adanya indikasi kebocoran data pribadi melalui media sosial. Ketika data kontak seluler yang berupa nomor telepon telah diunduh, maka pelaku akan menelpon calon korbannya. Cara lainnya adalah mengirim SMS berupa nomor undian dan meminta calon korban untuk menghubungi nomor telepon yang tertera dalam *body* SMS.

Tahap Membangun Kepercayaan (*Establishing Trust*) adalah tahap dimana pelaku mengembangkan hubungan dengan target atau calon korban guna membangun kepercayaan yang baik sehingga meningkatkan kepercayaan terhadap pelaku kejahatan. Apabila pelaku

melakukan telepon *direct* ke calon korban, maka pelaku akan berpura-pura memperkenalkan diri dan berusaha mengulur waktu dengan cara mendominasi arah pembicaraan dengan calon korban. Tahap Manipulasi Psikologi (*Psychological Manipulation*) adalah tahapan dimana pelaku menggunakan kepercayaan yang diperoleh untuk mendapatkan sebanyak mungkin informasi rahasia dari calon korban. Dalam kasus penipuan berkedok hadiah undian, pelaku sedapat mungkin meyakinkan calon korban bahwa hadiah undian tidak bisa diwakilkan dan harus diklaim sesegera mungkin. Pada umumnya, hadiah undian yang diiming-imingkan adalah hadiah yang bersifat fantastis seperti mobil, motor, ataupun hadiah uang yang bernilai jutaan rupiah. Dengan cara seperti ini, pelaku kejahatan yakin bahwa calon korban akan tergiur untuk mendapatkan hadiah undian tersebut. Setelah itu, dengan menggunakan alasan terkait pajak hadiah, pelaku meminta calon korban untuk segera mengklaim hadiah tersebut dan apabila tidak diklaim, maka akan dinyatakan hangus. Umumnya, pelaku tetap mendominasi pembicaraan telepon, berusaha tetap menunjukkan empati dan bersikap ramah terhadap setiap pertanyaan yang diajukan oleh calon korban.

Sedangkan Tahap Eksekusi (*The Exit*) adalah tahapan dimana pelaku kejahatan menemukan jalan keluar yang jelas sehingga tidak menimbulkan kecurigaan. Pelaku kejahatan sedapat mungkin memastikan bahwa tidak ada bukti apapun yang tertinggal yang dapat menyebabkan kerugian terhadap pelaku. Dalam kasus penipuan online berkedok hadiah undian, umumnya pelaku meminta calon korban untuk melakukan transfer via ATM dan tidak menganjurkan melalui *teller* perbankkan dengan upaya agar jejak transfer tidak dapat dilacak oleh pihak berwenang jika terjadi pelaporan tindak kejahatan penipuan oleh korban. Apabila calon korban berhasil melakukan transfer ke rekening tujuan dengan harapan mendapatkan undian hadiah, maka dalam proses ini, pelaku kejahatan telah berhasil menjalankan aksi kejahatan. Tindakan umum yang cenderung digunakan pelaku kejahatan adalah meniadakan nomor seluler yang telah digunakan sebelumnya.

Dengan menggunakan modus operasi yang telah disebutkan di atas dalam contoh kasus penipuan yang berkedok hadiah undian, metode pendekatan *sosio engineering* menjadi sangat efektif. Banyak unsur-unsur pendukung yang menjadikan metode ini berhasil dilakukan, seperti ketidaktahuan ataupun rasa kurang peka dari calon korban. Pada umumnya, tingkatan finansial ekonomi yang menjadi sasaran penipuan berada pada level ekonomi menengah ke bawah dan tingkat pendidikan yang cenderung rendah.

Mengacu kepada jumlah kejahatan *cyber* di Indonesia, banyaknya jumlah kasus terjadi dengan nilai yang fluktuatif namun memiliki kecenderungan kenaikan angka statistik. Berdasarkan *release* berita yang diterbitkan oleh media-media terpercaya, maka dapat dijabarkan sebagai berikut :

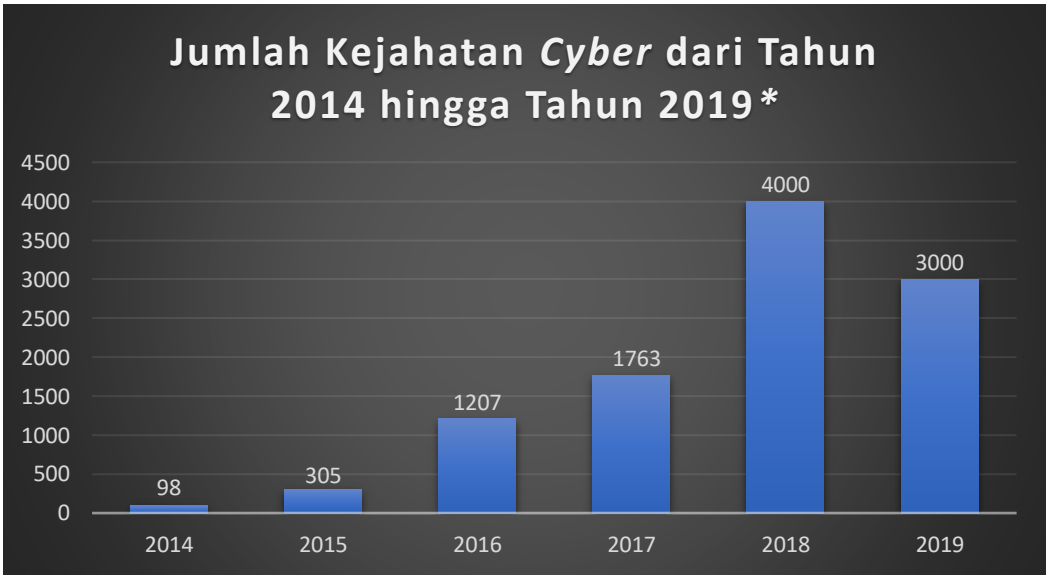
1. *Release* berita yang dikeluarkan oleh Koran Sindo dengan judul Kejahatan *Cyber Crime* Naik 300% pada Desember 2015 (Yuhandi, 2015), jumlah kejahatan *cyber* tahun 2014 sebanyak 98 jumlah kasus dan tahun 2015 sebanyak 305 kasus, atau naik sekitar 300% (Yuhandi, 2015) dari tahun sebelumnya.
2. *Release* berita yang dikeluarkan oleh CNN Indonesia dengan judul *Cyber Crime*, Kasus Kejahatan Terbanyak di 2016 pada Desember 2016 (Dwi Ratnasari, 2016), jumlah kejahatan *cyber* pada tahun 2016 sebanyak 1.207 jumlah kasus.
3. *Release* berita yang dikeluarkan OkeNews dengan judul Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber pada Desember 2017 (Batubara, 2017), jumlah kejahatan *cyber* pada tahun 2017 sebanyak 1.763 jumlah kasus.
4. *Release* berita yang dikeluarkan Detik Finance dengan judul 4.000 Laporan *Cyber Crime*, Mayoritas Korbannya Perusahaan pada Januari 2019 (Sugianto, 2019), jumlah kejahatan *cyber* pada tahun 2018 sebanyak 4.000 jumlah kasus.
5. *Release* berita yang dikeluarkan oleh CNN Indonesia dengan judul Polri Catat 3.000 Kasus Kejahatan Siber Hingga Agustus 2019 pada Oktober 2019 (CNN Indonesia, 2019), tercatat bahwa dalam rentang waktu Januari 2019 hingga Agustus 2019 jumlah kejahatan *cyber* tercatat sebanyak 3.000 kasus.

Apabila gambarkan dalam bentuk grafik statistik berdasarkan pada *release* berita yang diterbitkan oleh media massa ternama, maka akan terlihat dengan jelas, bahwa terjadi kenaikan angka terkait jumlah kejahatan *cyber* dari tahun 2014 hingga pertengahan tahun 2019. Penulis mengumpulkan hasil data jumlah kejahatan *cyber* yang dikeluarkan oleh media massa dan menggambarkannya dalam pola statistik berupa tabel dan gambar untuk memudahkan pendeskripsian kenaikan angka yang terjadi dari tahun ke tahun. Adapun jumlah kenaikan angka berdasarkan *press release* yang dikumpulkan oleh penulis, diperlihatkan dalam Tabel 1 dan Gambar 5.

Tabel 1. Jumlah Kejahatan *Cyber* dari Tahun 2014 hingga Tahun 2019*****

Jumlah Kejahatan *Cyber* dari Tahun 2014 hingga Tahun 2019*						
	2014	**2015**	**2016**	**2017**	**2018**	**2019***
Total Jumlah Kasus	98	305	1207	1763	4000	3000

*******Januari sampai Agustus 2019*



Gambar 5. Grafik Peningkatan Jumlah Kejahatan *Cyber* dari 2014 hingga 2019 (Januari sampai Agustus 2019)

Tidak dapat disangkal bahwa dengan kemajuan teknologi dapat menambah alur panjang kejahatan *cyber* yang ikut berevolusi bersama dengan kemajuan teknologi. Diperlukan kebijakan dari pemerintah tentang pentingnya perlindungan dalam bentuk undang-undang khususnya undang-undang ITE terkait hal-hal yang mencakup kejahatan *cyber* di Indonesia, terlebih mengenai undang-undang Perlindungan Data Pribadi. Undang-undang Perlindungan Data Pribadi (PDP), yang masih dalam proses perancangan undang-undang (RUU), diharapkan mampu menjawab problematika terkait kejahatan *cyber* di Indonesia (DPR/MPR RI, 2019) (Palinggi & Allolinggi, 2019). Dalam persepsi penulis, hukum yang bersifat melindungi adalah hukum yang dapat memberikan efek jera kepada pelaku sehingga tindak kejahatan *cyber* tidak terulang kembali oleh pelaku yang sama pula dikemudian hari.

KESIMPULAN

Dengan adanya kemajuan-kemajuan teknologi seperti *Fifth Generation*, *High Throughput Satellite*, *High Altitude Platform Station*, *Artificial Intelegent*, *Blockchain* hingga *Big Data*, maka secara tidak langsung memberikan persepsi bahwa era *Society 4.0* akan segera berakhir dan digantikan oleh era *Society 5.0*. Pola kejahatan *cyber* ikut berevolusi mengikuti perkembangan dari teknologi. Salah satu metode yang digunakan dalam kejahatan *cyber* adalah metode pendekatan *sosio engineering* dimana pelaku melakukan tindak atau praktek menipu seseorang, baik secara langsung, melalui telepon, atau menggunakan komputer, dengan tujuan untuk mengambil data atau informasi yang penting. Dan hasilnya adalah terjadinya peningkatan kasus kejahatan *cyber* dari tahun ke tahun khususnya kasus terkait penipuan berkedok hadiah undian. Diperlukan sebuah tindak pidana yang tepat untuk mengurangi resiko terjadinya kasus kejahatan *cyber* dengan cara memberikan efek jera kepada para pelaku kejahatan. Jadi perilaku kejahatan *cyber* ikut berkembang seiring dengan perkembangan teknologi yang semakin canggih.

DAFTAR PUSTAKA

APJII. (2018). Responden Survei Nasional Penetrasi Pengguna Internet 2018. Dikutip dari *Asosiasi Penyelenggara Jasa Internet Indonesia*. Dikutip dari www.apjii.or.id

Ariansyah, K. (2015). Proyeksi Jumlah Pelanggan Telepon Bergerak Seluler di Indonesia. *Buletin Pos Dan Telekomunikasi*, *12*(2), 151–166. https://doi.org/10.17933/bpostel.2014.120206

Batubara, P. (2017). Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber. Dikutip dari Oke News website: https://nasional.okezone.com/read/2017/12/21/337/1833784/tahun-2017-polisi-tangani-1-763-kasus-kejahatan-siber (Diakses pada 25 Desember 2019)

BSSN. (2018). Badan Sandi dan Siber Negara. Dikutip dari Badan Sandi dan Siber Negara website: www.bssn.go.id (Diakses pada 25 Desember 2019)

Bungin, B. (2011). Penelitian Kualitatif: Komunikasi, Ekonomi, Kebijakan Publik, Dan Ilmu Sosial Lainnya. Dikutip dari *Kencana*. https://doi.org/10.1002/jcc.21776

CNN Indonesia. (2019). Polri Catat 3.000 Kasus Kejahatan Siber Hingga Agustus 2019. Dikutip dari CNN Indonesia website: https://www.cnnindonesia.com/teknologi/20191029183819-185-443890/polri-catat-3000-kasus-kejahatan-siber-hingga-agustus-2019 (Diakses pada 25 Desember 2019)

Detikinet. (2014). Kronologi Penipuan Online yang Dialami Roy Suryo. Dikutip dari Detikinet website: https://inet.detik.com/cyberlife/d-2682136/kronologi-penipuan-online-yang-dialami-roy-suryo (Diakses pada 25 Januari 2020)

Dinesh, S. (2014). Social Engineering: The Human Factor. *Fatigue Assessment of Welded Joints by Local Approaches*, 1–13. https://doi.org/10.1016/b978-1-85573-948-2.50017-2

DPR/MPR RI. (2019). *Rancangan Undang-Undang Republik Indonesia Tentang Perlindungan Data Pribadi*. (1), 1–41. Dikutip dari https://aptika.kominfo.go.id/wp-content/uploads/2019/09/RUU-PDP.pdf

Dwi Ratnasari, E. (2016). Cyber Crime, Kasus Kejahatan Terbanyak di 2016. Dikutip dari CNN Indonesia website: https://www.cnnindonesia.com/nasional/20161230232449-12-183255/cyber-crime-kasus-kejahatan-terbanyak-di-2016 (Diakses pada 25 Desember 2019)

Fauzi, F., Harly, G. S., & Hs, H. (2012). Analisis Penerapan Teknologi Jaringan Lte 4G Di Indonesia. *Majalah IImilah UNIKOM*, *10*(2), 281–290.

Government of Japan. (2018). Realizing Society 5.0. Dikutip dari Japan Government website: https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf (Diakses pada 25 Januari 2020)

I-Scoop. (2017). From Industry 4.0 to Society 5.0: the Big Societal Transformation Plan of Japan. Dikutip dari I-Scoop website: https://www.i-scoop.eu/industry-4-0-society-5-0/ (Diakses pada 25 Januari 2020)

Junaedi, D. I. (2017). Antisipasi Dampak Social Engineering Pada Bisnis Perbankan. *Infoman's*, *11*(1), 1–10. https://doi.org/10.33481/infomans.v11i1.13

Keidanren. (2016). Toward Realization of The New Economy and Society. *Policy & Action* (Vol. 2016). Dikutip dari http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf

Kominfo. (2016). *Kelayakan Implementasi High Altitude Platforms (HAPs): Studi Kasus Project Loon*. Jakarta, Indonesia.

Lidwina, A., & Fitra, S. (2019). Penipuan Online, Kejahatan Siber yang Paling Banyak Dilaporkan. Dikutip dari Kata Data website: https://databoks.katadata.co.id/datapublish/2019/10/31/penipuan-online-kejahatan-siber-paling-banyak-dilaporkan (Diakses pada 25 Desember 2019)

Palinggi, S., & Allolinggi, L. R. (2019). Analisa Deskriptif Industri Fintech di Indonesia: Regulasi dan Keamanan Jaringan dalam Perspektif Teknologi Digital. *Ekonomi Dan Bisnis UPNVJ*, *6*(2), 177–192. https://doi.org/10.35590/jeb.v6i2.1327

Pilliang, Y. (2012). Masyarakat Informasi dan Digital: Teknologi Informasi dan Perubahan Sosial. *Jurnal Sosioteknologi*, *11*(Desember), 143–155.

Prima, E. (2019). Mengenal Visi Jepang Society 5.0: Integrasi Ruang Maya dan Fisik. Dikutip dari Tempo website: https://tekno.tempo.co/read/1170120/mengenal-visi-jepang-society-5-0-integrasi-ruang-maya-dan-fisik (Diakses pada 25 Januari 2020)

Qomariastuti, N. (2009). Pengaruh Rezim Internasional Terhadap Liberalisasi Sektor Telekomunikasi di Indonesia 2000-2008 (Universitas Indonesia). https://doi.org/10.1016/B978-008044910-4.00167-X

Saleh, G., & Arif, M. (2018). Rekayasa Sosial dalam Fenomena Save LGBT. *Jurnal Komunikasi Global*, *6*(2), 148–163.

Suciati Saputri, D., & Indrawan, A. (2015). Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber. Dikutip dari Republika website: https://www.republika.co.id/berita/nasional/umum/15/04/09/nmjajy-indonesia-peringkat-ke2-dunia-kasus-kejahatan-siber (Diakses pada 25 Desember 2019)

Sugianto, D. (2019). 4.000 Laporan Cyber Crime, Mayoritas Korbannya Perusahaan. Dikutip dari Detik Finance website: https://finance.detik.com/bursa-dan-valas/d-4398592/4000-laporan-cyber-crime-mayoritas-korbannya-perusahaan (Diakses pada 25 Desember 2019)

Suherman, Widodo, P., & Gunawan, D. (2017). Efektivitas Keamanan Informasi dalam Menghadapi Ancaman Social Engineering. *Jurnal Prodi Peperangan Asimetris*, *3*(April), 73–90.

Wardiana, W. (1994). Perkembangan Teknologi Informasi di Indonesia. *European Archives of Psychiatry and Clinical Neuroscience*, *243*(5), 224–228. https://doi.org/10.1007/BF02191578

Yuhandi, L. (2015). Kejahatan Cyber Crime Naik 300%. Dikutip dari Koran Sindo website: http://koran-sindo.com/page/news/2015-12-31/6/40/Kejahatan_Cyber_Crime_Naik_300_ (Diakses pada 25 Desember 2019)