e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 9 No 6 Tahun 2022 Hal. : 2043-2054

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

PENINGKATAN KORBAN KEJAHATAN SIBER SELAMA PANDEMI COVID19

Muhammad

Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia

Abstrak

Situasi pandemi mengubah cara dan gaya hidup sebagian besar masyarakat di Indonesia, dari yang sebelumnya tidak terlalu banyak melakukan pekerjaan secara online berubah dan terpaksa mengoptimalkan penggunaan teknologi. Kejahatan siber meningkat, pengkajian yang dapat digunakan seperti space transition theory, victim precipitation and participation, teori motivasi, teori existensialisme para pemikir postmodern, penyabaran informasi yang berkaitan dengan konspirasai dengan teori konspirasi yang berkembang di tengah media informasi, teori kontrol sosial, teori aktivitas rutin, teori kejahatan situasional, serta teori pengendalian diri yang rendah. Secara khusus, rendahnya tingkat pengendalian diri telah ditemukan terkait dengan di berbagai kejahatan seperti pembunuhan, viktimisasi properti dan kekerasan, penipuan dan viktimisasi kejahatan dunia maya (Bossler & Holt, 2010). Pengendalian diri yang rendah dari pelaku maupun korban memungkinkan terjadinya cyber victimization. Analisa kasus yang diberikan yaitu peningkatan kejahatan siber dengan teknik serangan phising dan hoax, teori konspirasi, dan media informasi sebagai platform kejahatan siber.

Kata Kunci: covid19, hoax, kejahatan siber, korban, teknologi.

PENDAHULUAN

Dinamisnya teknologi dengan perkembangannya yang pesat dan tak

*Correspondence Address : muhammad95@ui.ac.id
DOI : 10.31604/jips.v9i6.2022.2043-2054

kunjung henti merupakan suatu fenomena yang kita harus terima. Perkembangan inilah yang perlu kita ketahui dan sikapi terdapat pula kejahatan yang secara fisik tidak terlihat namun didalam dunia maya terjadi. Kejahatan dunia maya ini popular dengan beberapa tipe dan metode serangan yang dilakukan oleh para *cracker*. Kejahatan dunia maya yang popular saat ini adalah kejahatan yang memanfaatkan sisi kemanusiaan dari tiap individu. Dapat kita lihat sendiri di Indonesia terdapat laporan-laporan yang dilakukan langsung oleh para masyarakat (Patroli Siber, 2019).

Sepanjang penulisan terjadi pandemi yang berlangsung dan menimpa seluruh masyarakat dunia yaitu pandemi virus COVID19. Pada COVID19 sendiri jika dilihat secara global, virus ini merupakan penyakit menular yang disebabkan oleh jenis corona virus yang baru. COVID19 sendiri secara penelitian awal terjadi wabah di Wuhan, Tiongkok, bulan Desember 2019 (WHO, 2019). Hal ini memang akan menjadi tantangan sendiri untuk dunia global dan tiap negara dalam menyikapinya. COVID19 memberikan fenomena di tiap ruang lingkup masyarakat mulai dari negara, institusi, masyarakat hingga tiap individu itu sendiri.

Teknologi digital menyediakan konektivitas ini dan memberikan banyak manfaat kepada penggunanya. Tetapi pada saat yang sama, ia menyediakan lingkungan yang kaya untuk kegiatan kriminal, mulai dari perusakan hingga pencurian identitas hingga pencurian informasi pemerintah rahasia, Hal ini pulalah yang menjadi landasan penulis untuk melakukan penelitian kejahatan siber di tengah pandemi COVID19. Penelitian yang dilakukan memanfaatkan informasi dan kepustakaan yang dikumpulkan berdasarkan riset-riset sebelum COVID19 dan selama COVID19 berlangsung sehingga hasil yang diharapkan akan menggambarkan situasi kejahatan siber khususnya pada masyarakat Indonesia dan secara umum pada dunia.

METODE PENELITIAN

Metode penelitian yang digunakan oleh penulis dalam penelitian ini adalah dengan menggunakan pendekatan kualitatif. Penelitian dengan pendekatan kualitatif yang digunakan adalah dengan pengumpulan informasi dan literatur. Dari data tersebut kemudian akan dianalisa sehingga akan didapatkan pemaparan terkait dengan kondisi kejahatan siber.

Berbagai informasi dan literatur yang digunakan diambil dari situasi kejahatan siber sebelum dan disaat berlangsungnya pandemi covid19. Literatur yang digunakan dibatasi berdasarkan 10 tahun terakhir untuk menggambarkan kondisi terbaru yang mungkin juga akan mengalami perubahan setelah adanya pandemic covid19 yang berlangsung.

Pada situasi pandemi meningkat berita atau informasi yang tidak benar (hoax), dan serangan-serangan siber juga mengalami peningkatan, pembahasan yang dilakukan penulis membatasinya terkait dengan serangan yang menyerang individu seperti phising dan hoax dengan keterkaitanannya bersama dengan teori konspirasi yang beredar dan media informasi sebagai platform kejahatan siber.

HASIL DAN PEMBAHASAN

Untuk mempermudah pemahaman dan menghindari salah pengertian terhadap kondisi yang ada maka penulis memberikan deskripsi dari cybercrime, kondisi dari cybercrime selama covid19 dan analisa dari kejahatan siber sesuai batasan yang penulis sampaikan yaitu phising dan hoax pada masa pandemi sesuai dengan teori korban dan teori yang terkait serta penganalisannya sesuai pandangan

kriminologi sebagai salah satu bidang keilmuan yang penulis sedang tekuni.

1. Cybercrime

Florida Tech Online merilis permulaan percobaan kejahatan pada sistem komputer dan pengguna. Pada kenyataan ini kita dapat melihat Hubungan jahat dengan peretasan menjadi jelas pada 1970-an ketika sistem telepon komputerisasi awal menjadi sasaran. Orang-orang yang paham teknologi, yang disebut "*phreakers*" menemukan kode dan nada yang benar yang akan menghasilkan layanan jarak jauh gratis. Mereka menyamar sebagai operator, menggali melalui perusahaan Bell Telephone untuk menemukan informasi rahasia, dan melakukan eksperimen yang tak terhitung jumlahnya pada perangkat keras telepon awal untuk mempelajari cara mengeksploitasi sistem. Mereka adalah peretas dalam segala hal, menggunakan akal mereka untuk memodifikasi perangkat keras dan perangkat lunak untuk mencuri waktu telepon jarak jauh (Florida Tech Online, 2019).

Terdapat tantangan sendiri dalam *cyber crime* sesuai dengan *routine activity theory* yaitu: "*a supply of motivated offenders; the availability of suitable opportunities and the absence of capable guardians"* (Clough, 2015). Pada kejahatan siber kita akan mendapati teori transisi ruang (*Space Transition Theory*) yang dikemukakan oleh Jaishankar. Teori ini menjelaskan tentang sifat perilaku orang-orang yang mengeluarkan perilaku menyesuaikan diri dan tidak menyesuaikan diri dalam ruang nyata dan maya (Jaishankar, 2018).

Keamanan sistem informasi menjadi topik yang penting untuk dibahas, karena pada pandemi berlangsung terjadi perubahan yang signifikan dari aktivitas yang memanfaatkan teknologi secara penuh. Pada kompleksitas permasalahan keamanan informasi sendiri terbagi menjadi dua bagian utama, yaitu keamanan sistem dan keamanan pengguna (Senie Destya, 2018).

Pelaku *cyber crime* termotivasi dengan menilai kesesuaian dan daya tarik target online dan kemungkinan besar melakukan pelanggaran ketika tidak ada perwalian atau aturan yang mampu menelaah kejadian-kejadian di dunia maya Mereka juga mengatakan Pengguna harus menyadari bahwa aktivitas online tertentu, misalnya: menghabiskan terlalu banyak waktu untuk berbelanja dan perbankan online, menonton gambar dan video yang mungkin mengandung *malware*, bermain video game, mengunduh musik dan media yang mungkin memiliki virus, dan mengakses media sosial, mengobrol di kamar online, forum, dan obrolan akan meningkatkan visibilitas online mereka secara tidak proporsional. Interaksi selanjutnya dengan pelaku potensial akan membuat mereka berisiko menjadi target yang cocok di dunia maya (Ming-Li Hsieh & Shun-Yung Kevin Wang, 2018).

terdapat 4 tipe umum kejahatan siber terkait dengan hubungan komputer dengan kejahatan itu sendiri: 1) Komputer sebagai sasaran, pencurian kekayaan intelektual, pencurian informasi pemasaran (misalnya, daftar pelanggan, data harga, atau rencana pemasaran), dan pemerasan berdasarkan informasi yang diperoleh dari file yang terkomputerisasi (misalnya, informasi medis, riwayat pribadi, atau preferensi seksual), 2) Komputer sebagai perangkat kejahatan: penipuan dalam penggunaan kartu dan rekening ATM, pencurian uang dari akun akrual, konversi, atau transfer, penipuan kartu kredit, penipuan dari transaksi komputer (transfer saham, penjualan, atau penagihan)), dan penipuan telekomunikasi, 3) Komputer bersifat insidental terhadap kejahatan lainnya: pencucian uang dan transaksi perbankan yang melanggar hukum, catatan atau

buku kriminal terorganisir, dan pembuatan buku, 4) kejahatan terkait dengan prevalensi komputer: pembajakan / pemalsuan perangkat lunak, pelanggaran hak cipta atas program komputer, peralatan palsu, peralatan dan program komputer pasar gelap, dan pencurian peralatan teknologi (Jahankhani, 2014).

2. Cybercrime Selama Covid19

Berbicara mengenai *cyber crime* selama pandemi covid19, Indonesia telah membentuk badan keamanan siber yang berada pada naungan BSSN (Badan Siber dan Sandi Negara). BSSN melaporkan terdapat 88 juta serangan siber selama covid19 berlangsung. Pada 1 Januari hingga 12 April 2020 88.414.296 serangan siber yang terjadi di Indonesia. Puncak terbanyak terdapat pada bulang Februari yaitu 29.188.645 serangan yang terjadi. Klasifikasi yang diinformasikan yaitu terdapat 5 terbanyak serangan siber pada masa pandemi. 5 serangan tersebut ialah Trojan Activity, *Information Gathering*, Exploit Kit, Policy Violation dan Web Application Attack. Jika dilihat pada serangan yang ada ini semua lebih mengarah kepada sebuah sistem dan berdasarkan laporan yang ada 2 terbanyak ialah Trojan Activity 56% dan *Information Gathering* dengan besaran 43% (BSSN, 2020).

WHO sendiri merilis keterangan untuk masyarakat dunia agar berhati-hati dengan serangan siber yang dilakukan oleh para pelaku kejahatan siber, pada situsnya WHO merilis bahwa mungkin beberapa pelaku melakukan *phising* untuk menjadikan masyarakat dunia sebagai korban dengan pandemi covid19 yang sedang berlangsung. Email "*Phishing*" ini tampaknya berasal dari WHO, dan akan meminta korban untuk: memberikan informasi sensitif, seperti nama pengguna atau kata sandi klik tautan jahat membuka lampiran jahat. Dengan menggunakan metode ini, penjahat dapat menginstal *malware* atau mencuri informasi sensitif (WHO, 2020).

Selain serangan terhadap individu di dunia, terdapat pula penyebaran informasi hoax yang merajalela dan mengaburkan informasi yang tidak harusnya di terima oleh masyarakat dunia. Indoenesia melalui Kominfo seperti yang dirilis oleh detik news mengatakan 554 hoax yang tersebar di tengah pandemi virus Corona (COVID-19), hoax tersebut tersebar di platform digital, seperti Facebook, Instagram, Twitter, dan YouTube (Detik News, 2020).

Sesuai dengan yang telah tersampaikan peningkatan kejahatan siber selama pandemi covid19 menyerang seluruh individu, instansi, negara dan komunitas internasional. Penulis akan menekankan pada peristiwa kasus *phising* yang berdasarkan laporan BSSN sendiri meningkat dan merupakan kejahatan yang umum dilakukan namun tetap menghasilkan korban dengan jumlah yang cukup banyak secara signifikan. Selain metode *phising*, penulis memberi analisa lain terkait dengan kasus hoax atau kejahatan dengan media informasi sebagai platformnya.

3. Peningkatan Phising Selama Covid 19

Rekayasa sosial didefinisikan sebagai metode yang berupaya mengeksploitasi kelemahan dalam sifat manusia dan memanfaatkan kenaifan orang kebanyakan. Meskipun teknik rekayasa sosial telah berkembang dari waktu ke waktu, keberhasilan serangan seperti itu masih tergantung pada alat pencegahan modern dan sistem keamanan yang ada, serta ketersediaan personel terlatih dan terampil yang menangani data sensitif dalam organisasi (Sallai, 2016). Didalam serangan *social engineering* dikenal istilah *phising* yaitu: “sebagai tindakan mengirim email berbahaya yang berpura-pura berasal

dari sumber yang memiliki reputasi baik. Tujuan *phising* dapat dirinci sebagai berikut: (1) Untuk mengirim muatan berbahaya yang memberikan akses ke penyerang jarak jauh, (2) Untuk mengumpulkan kredensial, (3) Untuk mengumpulkan bit intel lainnya untuk serangan lebih lanjut" (Hadnagy, 2018:229).

Pada konsep keamanan informasi dipengaruhi oleh tiga faktor, masing-masing dijelaskan terjadinya rekayasa sosial sebagai berikut: 1) Proses: Suatu sistem keamanan dibangun dengan menggunakan dokumen resmi perusahaan yang berupa standar, prosedur, maupun kebijakan. Kebijakan yang dimiliki oleh perusahaan inilah yang akan menjadi landasan utama dalam keamanan informasi, di mana kebijakan tentang keamanan informasi sebaiknya harus ditandatangani oleh pimpinan puncak dari suatu perusahaan. Dengan adanya penandatanganan dari pimpinan puncak akan menandakan bahwa pimpinan sudah menyetujui adanya kebijakan tersebut dan menjadikannya sebagai prioritas utama dari perusahaan yang harus diikuti oleh semua karyawan perusahaan tersebut. Karena itulah dalam keamanan informasi, suatu kebijakan menjadi urutan pertama yang harus diprioritaskan. 2) Manusia: Sebuah sistem dijalankan oleh manusia sebagai penggunanya. Akan tetapi seperti yang dikemukakan oleh Prof. Richardus Eko lndrajit, dalam sebuah jaringan keamanan manusia menjadi bagian terlemah dalam sistem tersebut. Oleh karena itulah dalam keamanan informasi, manusia menjadi prioritas kedua yang harus diperhatikan. Ditambah lagi dalam aspek inilah yang akan menjadi sasaran utama dari Social Engineer Hacker. 3) Teknologi: Meskipun saat berbicara mengenai sebuah keamanan jaringan selalu menyinggung tentang teknologi, akan tetapi aspek ini menjadi urutan ke tiga yang harus diprioritaskan. Aspek teknologi yang dapat digunakan untuk keamanan jaringan dapat berupa pemasangan/penyettingan firewall untuk mengatur keluar masuknya transmisi di dalam jaringan, anti-virus, anti-spam, Intrusion Detection System untuk mendeteksi keanehan di dalam jaringan, maupun Intrusion Prevention System sebagai pencegahan jika ada terjadi penyerangan, (Rafzan, 2016).

Pada proses rekayasa sosial terdaoat fase pre-attack session terkait yang didapati serangan tersebut dengan sebaran terbanyak pada email 32%, aplikasi obrolan 44%, telepon 4%, sms 8%, tatap muka 8%, lainnya 4%. Pada *security and risk mitigation strategic framework* manusia berada pada faktir utama diantara proses dan teknologi. Untuk mengurangi jumlah korban pada kejahatan siber tiap individu, organisasi dan masyarakat dapat mengintervensi dan meningkatkan kesadaran, pendidikan, motivasi / rasa urgensi, kemampuan. Hal tersebut juga terkait dengan *human firewall* atau dinding pelindung diri sendiri, hal tersebut terkait dengan naluri, kebiasaan, tingkah laku dan kebudayaan (Indrajit, 2017).

4. Hoax, Teori Konspirasi, dan Media Informasi Sebagai Platform Kejahatan Siber

Sassasasas Hoax atau berita palsu menjadi fenomena yang berkembang ditengah dinamisnya kehidupan sosial. Hal ini dipermudah pula dengan keberadaan dari teknologi sebagai media komunikasi dan mencari informasi. Terdapat banyak peristiwa dari penyebaran informasi di Indonesia. Yang paling mudah dan saat ini sesuai dengan peristiwa yang dialami oleh masyarakat Indonesia dan bahkan dunia adalah penyebaran virus corona, COVID19 atau disebut juga dengan istilah n-Cov/SARS-COV-2. Hoax sendiri termasuk pada masalah cyber crime yang mana di Indonesia telah ada UU ITE

sebagai pondasi untuk menanggulangi permasalahan seperti ini. Namun, seiring perkembangan penerapan UU ITE didalam menanggulangi Hoax dan Ujaran Kebencian masih harus diperbaiki. Sebagai contoh terkait dengan permasalahan virus covid19 sendiri pemerintah pusat mencoba mengklarifikasi hoax-hoax yang berkembang di public. Tercatat pada 31 Mei 2020 terdapat 305 informasi hoax dan false information yang ditemukan terkait covid19 ini. Namun tidak heran hal ini sendiri terjadi karena adanya sistem politik terkait dengan cyber trooper atau buzzer politik yang jelas berperan dan dipelihara oleh negara kita sendiri. Berdasarkan penelitian dari Oxford 2019 dalam The Global Disinformation Order (2019 Global Inventory of Organised Social Media Manipulation) ditemukan Hoax sendiri diorganisasikan oleh para orang-orang dalam dunia politik dan partai serta private contractor yang menyediakan penyebaran informasi palsu. Strategi yang digunakan ialah memang memberikan disinformasi dan memanipulasi media, didalamnya ada peran bot serta manusia yang memproduksi hoax itu sendiri.

Pada pemikiran postmodern menunjukkan bahwa pasar media telah dideregulasi, yang mengarah ke dengan banyaknya program, judul, dan format yang dapat dipilih. Semua selera dan minat sekarang dapat dipenuhi, di mana konsumenlah yang pada akhirnya memiliki kekuatan untuk memilih apa yang dia tonton, dengarkan, baca, dan kerjakan, yang dengan jelas kekuatan tersebut memiliki kesamaan saat mereka mengabaikan atau menolak apa yang dia tolak. Oleh karena itu media masa dan runtuhnya setiap pemaknaan peristiwa menghasilkan budaya yang berpusat pada keinginan untuk mengonsumsi secara langsung. Terdapat dua ancaman yang tampak dari implikasi postmodern ini. Pertama, pasar media yang bersifat plural menggantungkan diri terhadap kemampuan publik membedakan antara yang benar dan yang tidak serta antara fakta dan interpretasi. Kedua, bagaimana posisi postmoderninsme dalam mendefinisikan hiburan yang mana kekerasan baik itu kejahatan dan kekerasan itu sendiri dianggap adalah upaya intrinsik menghibur penonton di mana beragam visualisasi lebih dimaknai secara emosional (Jewkes, 2016).

Seiring berkembangnya informasi dan media sendiri baik konvensional maupun online sendiri membantu penyebaran informasi dan dapat dikaitkan dengan teori konspirasi. Pada pandemi covid19 terdapat teori konspirasi yang digaungkan oleh beberapa penyuka maupun penelitinya sendiri. Hampir setengah dari warga Kanada mengikuti teori konspirasi virus korona - termasuk obat mujarab yang disangkal, gagasan tentang penutupan 5G atau bahwa virus itu direkayasa di laboratorium Tionghoa pada sebuah studinya. School of Journalism di Carleton University di Ottawa mensurvei 2.000 orang Kanada dan menemukan bahwa 46 persen percaya pada setidaknya satu dari empat mitos utama yang beredar secara online. Konspirasi pada COVID19 yaitu adanya rekayasa sebagai bio weapon di laboratorium Cina dan dilepaskan ke populasi umum – hal ini diyakini oleh 26 persen orang Kanada. 11 persen responden lainnya mengatakan bahwa mereka berpikir COVID-19 bukan penyakit serius tetapi disebarkan untuk menutupi dugaan dampak kesehatan yang berbahaya terkait dengan paparan teknologi nirkabel 5G. Para peneliti mencatat bahwa orang-orang yang menghabiskan banyak waktu di platform media sosial, termasuk Twitter, Instagram dan TikTok, kemungkinan besar akan percaya pada teori konspirasi (The Jakarta Post, 2020).

Terlepas benar atau tidaknya teori yang timbul di tengah pandemi covid19, konspirasi maupun teori

konspirasi tersebut menghasilkan korban. Pada teori konspirasi ketika dibandingkan dengan penjelasan non-konspirasi, individu mencoba mencari kepuasan dengan motif sosial-psikologis penting yang dapat dicirikan sebagai epistemik (misalnya, keinginan untuk memahami, akurasi, dan kepastian subyektif), eksistensial (misalnya, keinginan untuk kontrol dan keamanan), dan sosial (misalnya, keinginan untuk mempertahankan citra positif diri atau kelompok). Taksonomi ini, yang berasal dari teori justifikasi sistem Jost, Ledgerwood, & Hardin, 2008 (dalam Douglas, 2017) berfungsi sebagai heuristik yang berguna untuk mengklasifikasikan motif yang terkait dengan keyakinan konspirasi. Namun, penelitian yang relatif langka memeriksa konsekuensi dari teori konspirasi tidak menunjukkan bahwa mereka pada akhirnya membantu orang memenuhi motif ini.

Pada media dengan adanya hoax disertai dengan teori konspirasi sebagaimana ciri yang disampaikan oleh Douglas kita dapat menemukan penjelasan sebab akibat untuk peristiwa adalah bagian inti dari membangun pemahaman dunia yang stabil, akurat, dan konsisten secara internal Heider, 1958 (dalam Douglas, 2018). Motif-motif epistemik spesifik yang dapat dijelaskan oleh penjelasan sebab-akibat termasuk rasa penasaran yang meluap-luap ketika informasi tidak tersedia, mengurangi ketidakpastian dan kebingungan ketika informasi yang tersedia saling bertentangan, menemukan makna ketika peristiwa-peristiwa tampak acak, dan mempertahankan kepercayaan dari diskonfirmasi. Terkait dengan motif-motif ini, teori konspirasi memiliki atribut yang membedakan mereka dari jenis penjelasan sebab akibat lainnya. Meskipun dengan tingkat yang berbeda-beda, mereka spekulatif karena mereka menempatkan tindakan yang tersembunyi dari pengawasan publik, kompleks dalam hal mereka mendalilkan koordinasi berbagai aktor, dan tahan terhadap pemalsuan karena mereka berpendapat bahwa konspirator menggunakan *stealth* dan disinformasi untuk menutupi tindakan mereka. Lewandosky menyatakan bahwa orang yang mencoba mengingkari teori konspirasi dapat, dengan sendirinya, menjadi bagian dari konspirasi (Douglas, 2017).

Properti terkait teori konspirasi adalah bahwa mereka dapat melindungi kepercayaan yang dihargai (misalnya, vaksinasi berbahaya; perubahan iklim bukan masalah serius) dengan memberikan bukti yang sangat tidak dapat dikonfirmasi (misalnya, temuan ilmiah) sebagai produk konspirasi seperti yang disampaikan oleh Lewandowsky, Oberauer, & Gignac, 2013 (dalam Douglas, 2017). Secara umum, penjelasan yang dijamin secara empiris (vs spekulatif), sedikit (vs kompleks), dan yang dapat dipalsukan lebih kuat menurut standar normatif penjelasan kausal (misalnya, dalam sains). Namun, teori konspirasi tampaknya memberikan penjelasan yang luas dan konsisten secara internal yang memungkinkan orang untuk melestarikan kepercayaan dalam menghadapi ketidakpastian dan kontradiksi. Sesuai dengan analisis ini, penelitian menunjukkan bahwa kepercayaan pada teori konspirasi lebih kuat ketika motivasi untuk menemukan pola di lingkungan secara eksperimental meningkat seperti yang di sampaikan Whitson & Galinsky, 2008 (dalam Douglas, 2017). Hal ini diperkuat antara orang-orang yang terbiasa mencari makna dan pola di lingkungan, termasuk orang percaya pada fenomena paranormal. Tampak juga ketika peristiwa terutama dalam skala besar atau signifikan dan membuat orang tidak puas dengan penjelasan biasa, skala kecil seperti yang di sampaikan oleh Leman & Cinnirella, 2013 (dalam Douglas, 2017). Selain itu, kebutuhan untuk penutupan

kognitif dikaitkan dengan keyakinan pada teori konspirasi yang menonjol untuk acara yang tidak memiliki penjelasan resmi yang jelas seperti yang disampaikan oleh Marchlewska, Cichocka, & Kossowska, 2017 (dalam Douglas, 2017). Van Prooijen & Jostmann, 2013, penelitian menunjukkan bahwa kepercayaan konspirasi lebih kuat ketika orang mengalami kesulitan sebagai akibat dari perasaan tidak pasti (Douglas, 2017). Sehingga terlihat bahwa teori konspirasi dapat memuaskan beberapa motif epistemik dengan mengorbankan yang lain — misalnya, dengan melindungi keyakinan dari ketidakpastian sambil kurang cenderung akurat. Kelemahan epistemik dari teori konspirasi tampaknya tidak mudah terlihat oleh orang-orang yang tidak memiliki kemampuan atau motivasi untuk berpikir kritis dan rasional. Keyakinan konspirasi berkorelasi dengan tingkat berpikir analitik yang lebih rendah seperti yang disampaikan oleh Swami, Voracek, Stieger, Tran, & Furnham, 2014 (dalam Douglas, 2017) dan tingkat pendidikan yang lebih rendah oleh Douglas, Sutton, Callan, Dawtry, & Harvey, 2016 (dalam Douglas, 2017). Keterkaitan dengan kecenderungan untuk melebih-lebihkan kemungkinan peristiwa yang terjadi bersamaan oleh Brotherton & French, 2014 dan kecenderungan untuk memahami agensi dan intensionalitas di tempat yang tidak ada Douglas et al., 2016 (Douglas, 2017).

Motif existensi dapat dilihat sebagai mana dikemukakan oleh Goertzel tentang keyakinan konspirasi menunjukkan bahwa orang beralih ke teori konspirasi untuk kompensasi kepuasan ketika kebutuhan ini terancam, misalnya orang-orang yang tidak memiliki kontrol instrumental dapat diberikan rasa kompensasi untuk mengontrol oleh teori konspirasi, karena mereka menawarkan kesempatan untuk menolak narasi resmi dan merasa bahwa mereka memiliki akun alternatif. Selain itu Bost dan Prunier teori konspirasi mungkin menjanjikan untuk membuat orang merasa lebih aman sebagai bentuk tipuan, di mana individu yang berbahaya dan tidak dapat dipercaya diakui dan ancaman yang ditimbulkannya dikurangi atau dinetralkan (Douglas, 2017). Paparan eksperimental untuk teori konspirasi tampaknya segera menekan rasa otonomi dan kontrol orang. Studi yang sama ini menunjukkan bahwa hal itu membuat orang kurang cenderung untuk mengambil tindakan dalam jangka panjang, dapat meningkatkan otonomi dan kontrol mereka. Secara khusus, mereka kurang cenderung untuk berkomitmen pada organisasi mereka dan untuk terlibat dalam proses politik arus utama seperti pemilihan dan politik partai. Selain itu, paparan teori konspirasi dapat secara halus merongrong otonomi orang dengan cara lain. Douglas dan Sutton menunjukkan bahwa orang secara efektif dibujuk oleh materi pro-konspirasi tetapi tidak sadar bahwa mereka telah diyakinkan dan salah mengingat bahwa kepercayaan mereka yang sudah ada sebelumnya identik dengan kepercayaan baru mereka. Karena teori konspirasi menunjukkan bahwa hasil penting ada di tangan kekuatan jahat yang memiliki dan menggunakan kekuatan di luar batas yang sah, tidak akan mengejutkan jika penelitian lebih lanjut menunjukkan bahwa efeknya sering melemahkan (Douglas, 2017).

Lebih lanjut pada motif sosial sendiri, pada motif sosial hal ini dapat dilihat pada keinginan untuk memiliki dan mempertahankan citra positif diri dan kelompok. Para ahli berpendapat bahwa teori konspirasi menghargai diri dan kelompok dengan membiarkan kesalahan untuk hasil negatif yang dikaitkan dengan orang lain. Dengan demikian, mereka dapat membantu menegakkan citra diri dan kelompok sebagai kompeten dan bermoral tetapi

disabotase oleh orang lain yang kuat dan tidak bermoral (Douglas, 2017). Graeupner dan Coman menyampaikan pengucilan menyebabkan orang percaya pada takhayul dan teori konspirasi, sebagai bagian dari upaya untuk memahami pengalaman mereka (Douglas, 2017). Status obyektif rendah (vs tinggi) karena etnisitas mereka seperti yang disampaikan Crocker, Luhtanen, Broadnax, & Blaine, 1999 atau penghasilan Uscinski & Parent, 2014 lebih cenderung mendukung teori konspirasi (dalam Douglas, 2017). Orang-orang di sisi yang kalah (vs menang) dari proses politik juga nampaknya lebih percaya teori konspirasi seperti penyampaian Uscinski & Parent, 2014 (dalam Douglas, 2017). Keyakinan konspirasi menurut Imhoff dan Bruder juga dikaitkan dengan prasangka terhadap kelompok-kelompok kuat dan menurut Kofta dan Sedek mereka yang dianggap sebagai musuh (Douglas, 2017). Eksperimen menunjukkan bahwa paparan teori konspirasi mengurangi kepercayaan pada institusi pemerintah, bahkan jika teori konspirasi tidak berhubungan dengan institusi tersebut seperti yang disampaikan oleh Einstein & Glick dengan penambahan kekecewaan pada politisi dan ilmuwan menurut Jolley & Douglas (dalam Douglas, 2017). Oleh karena itu, penelitian empiris menunjukkan bahwa teori konspirasi berfungsi untuk mengikis modal sosial dan dapat, jika ada, menggagalkan kebutuhan orang untuk melihat diri mereka sebagai anggota berharga dari kolektif yang layak secara moral.

Pada covid19 setidaknya sudah ratusan tindak kejahatan yang berkaitan dengan penyebaran informasi sesat yang sudah diproses dan sudah mengalami penangkapan pada pelaku yang menyebarkan informasi sesat tersebut. Wakabareskrim Irjen Wahyu Hadiningrat mengatakan, dalam operasi tersebut Polri membentuk 6 satgas, yakni Satgas Deteksi, Satgas Pencegahan, Satgas Penanganan, Satgas Rehabilitasi, Satgas Gakkum, dan Satgas Banops. Sejauh ini jumlah kegiatan patroli siber sudah dilakukan sebanyak 9.062 kegiatan. Melakukan *take down* 2.471 akun dan pihaknya juga melakukan kegiatan penindakan sebanyak 105 kegiatan. Sehingga sudah terdapat 11.584 kegiatan dengan 107 tersangka di dalamnya. Selain dengan penindakan terhadap pelaku, Ketua Masyarakat Indonesia Anti Hoax, Septiaji Eko Nugroho menguraikan lima langkah sederhana yang bisa membantu dalam mengidentifikasi mana berita hoax dan mana berita asli. Langkah tersebut dapat dijelaskan sebagai berikut: 1) Hati-hati dengan judul provokatif: Berita hoax sering kali menggunakan judul sensasional yang provokatif, misalnya dengan langsung menudingkan jari ke pihak tertentu. Isinya pun bisa diambil dari berita media resmi, hanya saja diubah-ubah agar menimbulkan persepsi sesuai yang dikehendaki sang pembuat hoax. Oleh karenanya, apabila menjumpai berita dengan judul provokatif, sebaiknya Anda mencari referensi berupa berita serupa dari situs online resmi, kemudian bandingkan isinya, apakah sama atau berbeda. Dengan demikian, setidaknya Anda sebbagian pembaca bisa memperoleh kesimpulan yang lebih berimbang. 2) Cermati alamat situs: Untuk informasi yang diperoleh dari website atau mencantumkan link, cermatilah alamat URL situs dimaksud. Apabila berasal dari situs yang belum ter verifikasi sebagai institusi pers resmi -misalnya menggunakan domain blog, maka informasinya bisa dibilang meragukan. Menurut catatan Dewan Pers, di Indonesia terdapat sekitar 43.000 situs di Indonesia yang mengklaim sebagai portal berita. Dari jumlah tersebut, yang sudah ter verifikasi sebagai situs berita resmi tak sampai 300. Artinya terdapat setidaknya puluhan ribu situs yang

berpotensi menyebarkan berita palsu di internet yang mesti diwaspadai. 3) Periksa fakta: Perhatikan dari mana berita berasal dan siapa sumbernya? Apakah dari institusi resmi seperti KPK atau Polri? Sebaiknya jangan cepat percaya apabila informasi berasal dari pegiat ormas, tokoh politik, atau pengamat. Perhatikan ke berimbangan sumber berita. Jika hanya ada satu sumber, pembaca tidak bisa mendapatkan gambaran yang utuh. Hal lain yang perlu diamati adalah perbedaan antara berita yang dibuat berdasarkan fakta dan opini. Fakta adalah peristiwa yang terjadi dengan kesaksian dan bukti, sementara opini adalah pendapat dan kesan dari penulis berita sehingga memiliki kecenderungan untuk bersifat subyektif. 4) Cek keaslian foto Di era teknologi digital saat ini , bukan hanya konten berupa teks yang bisa dimanipulasi, melainkan juga konten lain berupa foto atau video. Ada kalanya pembuat berita palsu juga mengedit foto untuk provokasi pembaca. Cara untuk mengecek keaslian foto bisa dengan memanfaatkan mesin pencari Google, yakni dengan melakukan *drag-and-drop* ke kolom pencarian Google Images. Hasil pencarian akan menyajikan gambar-gambar serupa yang terdapat di internet sehingga bisa dibandingkan. 5) Ikut serta grup diskusi anti-hoax. Di Facebook terdapat sejumlah fanpage dan grup diskusi anti hoax, misalnya Forum Anti Fitnah, Hasut, dan Hoax (FAFHH), Fanpage & Group Indonesian Hoax Buster, Fanpage Indonesian Hoaxes, dan Grup Sekoci. Di grup-grup diskusi ini, netizen bisa ikut bertanya apakah suatu informasi merupakan hoax atau bukan, sekaligus melihat klarifikasi yang sudah diberikan oleh orang lain. Semua anggota bisa ikut berkontribusi sehingga grup berfungsi layaknya *crowdsourcing* yang memanfaatkan tenaga banyak orang. Terakhir jika telah melakukan langkah tersebut pengguna internet dapat melaporkan hoax tersebut melalui sarana yang tersedia di masing-masing media. Untuk media sosial Facebook, gunakan fitur Report Status dan kategorikan informasi hoax sebagai *hatespeech/harrasment/rude/threatening*, atau kategori lain yang sesuai. Jika ada banyak aduan dari netizen, biasanya Facebook akan menghapus status tersebut. Untuk Google, bisa menggunakan fitur feedback untuk melaporkan situs dari hasil pencarian apabila mengandung informasi palsu. Twitter memiliki fitur Report Tweet untuk melaporkan twit yang negatif, demikian juga dengan Instagram. Kemudian, bagi pengguna internet Anda dapat mengadukan konten negatif ke Kementerian Komunikasi dan Informatika dengan e-mail ke alamat: aduankonten(at)mail.kominfo.go.id. Masyarakat Indonesia Anti Hoax juga menyediakan laman data.turnbackhoax.id untuk menampung aduan hoax dari netizen. TurnBackHoax sekaligus berfungsi sebagai database berisi referensi berita hoax.

KESIMPULAN

Kejahatan siber dapat dikurangi, sebuah ketidak-mungkinan untuk menghilangkannya mengingat perkembangan dan kemajuan keilmuan baik dalam bidak sains dan sosial. Langkah-langkah yang dapat dilakukan tersebut harus di lakukan oleh tiap individu, organisasi, negara dan masyarakat dunia untuk melakukan pencegahan. Selain mencegah sebagaimana *framework* yang telah disampaikan manusia merupakan faktor utama yang lemah dengan adanya kejahatan siber itu sendiri. Peningkatan kesadaran harus terus dilakukan bersama, pendidikan terkait dengan teknologi yang berkembang setidaknya harus diikuti oleh tiap individu, motivasi/rasa urgensi wajib dimiliki pula oleh tiap individu, serta kemampuan dan kecakapan dalam menggunakan teknologi tersebut juga sudah pasti perlu

dimiliki. Selain dengan meningkatkan hal-hal yang ada pada individu, terkait dengan covid19 tersebut faktor *human firewall* atau dinding pelindung diri sendiri juga perlu diasah, hal ini terkait dengan naluri setiap individu yang berkembang seiring dengan kegiatan yang dilakukan oleh tiap individu.

DAFTAR PUSTAKA

Clough, J. (2015). Criminal copyright infringement. In *Principles of Cybercrime* (pp. 255-271). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139540803.009

Destya, S., 2018. *Model Pengukuran Tingkat Kesadaran Keamanan Informasi di Universitas AMIKOM Yogyakarta*. *Makalah*. Dalam: Seminar Nasional Teknologi Informasi dan Multimedia 2018.

Douglas, K. M., Sutton, R. M., & Cichocka, A. (2017). *The psychology of conspiracy theories*. *Current directions in psychological science*, *26*(6), 538-542.

Florida Tech Online, dengan laman https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/, diakses pada hari Minggu 6 Februari 2022

Hadnagy, S., (2018). *Social Engineering: The Science of Human Hacking.* John Wiley & Sons, Inc., Indianapolis, Indiana, 229.

Harian Media Online Detik News. Menkominfo: Ada 554 Isu Hoax soal COVID-19, 89 Orang Jadi Tersangka, dengan laman https://news.detik.com/berita/d-4982087/menkominfo-ada-554-isu-hoax-soal-covid-19-89-orang-jadi-tersangka, diakses pada hari Minggu 6 Februari 2022

Harian Media Online The Jakarta Post. *Half of Canadians fooled by COVID-19 conspiracy theories: Study*, dengan laman https://www.thejakartapost.com/news/2020/05/21/half-of-canadians-fooled-by-covid-19-conspiracy-theories-study.html, diakses pada hari Minggu 6 Februari 2022.

Hsieh, M., & Wang, SK., (2018). *Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree*. International Journal of Cyber Criminology – ISSN:0973-5089 January – June 2018. Vol. 12(1): 333–352. DOI: 10.5281/zenodo.1467935.

Indrajit, R.E. (2019). *Social Engineering Framework: Understanding the Deception Approach to Human Element of Security*. IJCSI International Journal of Computer Science Issues, Volume 14, Issue 2, March 2017. DOI: 10.20943/01201702.816

Jahankhani, Hamid & Al-Nemrat, A. & Hosseinian-Far, Amin. (2014). Cyber crime Classification and Characteristics. 10.1016/B978-0-12-800743-3.00012-8.

Jaishankar, K., *Cyber Criminology as an Academic Discipline: History, Contribution and Impact*. International Journal of Cyber Criminology – ISSN:0973-5089 January – June 2018. Vol. 12(1): 1–8. DOI: 10.5281/zenodo.1467308.

Jewkes, Y., (2016) *Media and Crime*, University of Bath, UK: Sage Publication Ltd, Chapter 1

Patroli Siber, dengan laman https://patrolisiber.id/statistic, diakses pada hari Minggu 6 Februari 2022.

Panda Security, dengan laman https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/ diakses pada hari Minggu 12 Februari 2022.

Rafizan, O. (2016) Analisis Penyerangan Social Engineering. Jurnal Penelitian Teknologi Informasi dan Komunikasi: Puslitbang Aptika & IKP Balitbang SDM Kominfo.

Sallai, G. *Social Engineering Audit and Security Awareness Programme*; KPMG: Amstelveen, The Netherlands, 2016.

WHO. (2020). *Beware of criminals pretending to be WHO*. dengan laman https://www.who.int/about/communications/cyber-security diakses pada hari Minggu 12 Februari 2022.