Borneo Educational Journal (Borju)
https://jurnal.fkip-uwgm.ac.id/index.php/Borju
E-ISSN: 2655-9323
August 2023, Vol. 5 No. 2

The Threat of Social Network Games in Indonesia

Ancaman Social Network Game di Indonesia

Sandy[1], Djoko Andoko[2], Poppy Setiawati Nurisnaeny[3], Mira Murniasari[4]
Sekolah Tinggi Intelijen Negara, Indonesia
Email: sandy0131.ss@gmail.com; djoko.andoko@stin.ac.id; poppysetiawati@gmail.com; miraathira@yahoo.com

Abstract
This research examines the potential threat through SNG in Indonesia. The theories of threat, social media, cyber, and network society are used to analyze the research problem through qualitative analysis. Data was obtained through interviews and literature studies. The results of the study show that the potential threat on SNG includes ideological threats in society, growing illegal and pornographic content, theft of personal data, illegal monitoring of user activities, online fraud, cyberbullying, inappropriate content, dependence, and cyber-attacks that threaten the activities of social network game users in Indonesia.
Keywords: Threat; Network Society; Social Network Game; Espionage.

Abstrak
Penelitian ini mengkaji potensi ancaman SNG di Indonesia. Teori ancaman, media sosial, siber, dan network society digunakan untuk menganalisis masalah penelitian melalui analisis kualitatif. Data diperoleh melalui wawancara dan studi pustaka. Hasil dari penelitian menunjukkan bahwa potensi ancaman pada SNG meliputi ancaman ideologi di masyarakat, konten ilegal, dan pornografi semakin berkembang, pencurian data diri, monitoring aktivitas pengguna secara ilegal, penipuan online, cyberbullying, konten-konten yang tidak pantas, ketergantungan, dan serangan cyber yang mengancam aktivitas pengguna social network game di Indonesia
Keywords: Ancaman; Network Society; Social Network Game; Spionase.

DOI	**:**	**doi.org/10.24903/bej.v5i2.1393**
Received	:	August 2023
Accepted	:	August 2023
Published	:	August 2023

1. PENDAHULUAN

Era digital bermanfaat besar melalui banyaknya platform yang tersedia di dalam jejaring (online) yang memberikan kemudahan bagi aktivitas manusia. Kemudahan tersebut di antaranya dalam mengakses informasi yang dibutuhkan untuk melakukan keseharian, baik dalam konteks kehidupan personal, professional, maupun dunia kerja. Namun, demikian perkembangan dunia tidak selalu memberikan efek yang positif, mengingat pola interaksi sosial yang berubah secara drastis juga diiringi dengan berbagai ancaman.

Berdasarkan tren perkembangan tersebut didukung dengan fakta bahwa data pengguna internet memang berkembang pesat dari hari ke hari. Kegiatan intelijen dalam bidang keamanan yang berkaitan dengan Open-Source Intelligence (OSINT) menjadi sesuatu yang sangat diperlukan oleh negara (Ivanjko, 2019). Adapun pemanfaatannya guna menjamin keamanan data warga negara mereka sekaligus keamanan nasional. Perlindungan terhadap keamanan data sangat penting dilakukan karena pada zaman modernisasi saat ini, semakin banyak kemudahan bagi pihak tertentu untuk melakukan pencurian data-data maupun informasi pribadi yang dimiliki individu lain. Kemudahan pencurian data tersebut disebabkan karena mudahnya mendapatkan informasi terkait personal atau individu di internet maupun media sosial. Informasi yang membantu pelaku dalam melakukan pencurian data disebut dengan Personally Identifiable Information (PII) atau Informasi Pengenal Pribadi (Narayanan, 2010).

Personally identifiable information adalah informasi-informasi yang dapat teridentifikasi secara pribadi oleh orang lain dan informasi tersebut merupakan bagian dari data-data yang dapat mengidentifikasi individu tertentu. PII juga merupakan informasi maupun data-data yang dapat digunakan untuk membedakan satu orang dari orang lain karena data PII ini dapat digunakan untuk menganonimkan data yang sebelumnya anonim di internet. Pelaku pencurian data yang mendapatkan data-data PII akan semakin mudah melakukan pencurian data milik orang lain karena banyaknya data yang relevan dengan informasi orang atau personal maupun individu. Oleh karena itu, PII merupakan data penting yang perlu diamankan oleh setiap individu (Schwartz, 2011).

Aktivitas untuk melindungi dan menjaga PII sangat penting dilakukan karena berfungsi dalam melindungi keamanan informasi, privasi informasi, perlindungan data, privasi data, dan privasi pribadi. Apabila pelaku pencurian data berhasil menemukan sedikit atau beberapa data yang dimiliki oleh pribadi seseorang yang dijadikan target, pelaku pencurian data dapat membuat akun palsu atas nama orang tersebut. Pelaku tersebut dapat memanfaatkan informasi untuk menjalankan kepentingan yang akan dilaksanakan oleh

pelaku pencurian data. Pelaku pencurian data bisa melakukan hal-hal ilegal yang merugikan individu tersebut seperti melakukan peminjaman uang, pembuatan paspor palsu, dan menjual identitas seseorang kepada pelaku pencurian data yang lain. PII juga bisa digunakan sendiri ataupun bersama-sama dengan data lain yang relevan untuk mengidentifikasi seseorang dan dapat menyertakan pengidentifikasian secara langsung untuk melakukan objektivitas atau keakuratan terhadap data-data yang diterima. Objektivitas yang dilakukan seperti penemuan informasi paspor yang dapat mengidentifikasi seseorang secara unik atau pengidentifikasian semu, penemuan informasi ras yang dapat digabungkan dengan kuasi dan identitas personal yang lainnya, penemuan informasi tanggal lahir yang dapat mengidentifikasi objektivitas bahwa berhasil mengenali seseorang. Pencurian data-data melalui pencurian data PII merupakan ancaman yang dapat membahayakan keamanan dan kedaulatan negara (Krishnamurthy, 2009).

Social network game merupakan bagian dari domain siber. Domain siber saat ini telah menjelma menjadi domain of warfare yang meski tidak kasat mata dan tidak memiliki bentuk fisik, dapat menimbulkan dampak fisik hingga psikis yang fatal karena melampaui batas ruang dan waktu. Sehingga menjadi sulit bagi negara untuk menegakan kedaulatan di dalam domain tersebut. Berpijak dari penjelasan di atas, penelitian ini disusun dengan berfokus pada perkembangan dari social network game yang diasumsikan dapat berpotensi menjadi ancaman spionase dari negara maupun aktor non negara lain terhadap Indonesia. Hal ini dipandang penting untuk diteliti dari perspektif intelijen karena adanya potensi ancaman melalui platform digital, khususnya pada social network game yang dapat berdampak pada kepentingan dan keamanan nasional.

Keberadaan social network game dapat membantu masyarakat khususnya generasi muda di Indonesia untuk membentuk kebiasaan bertanggung jawab, ramah, visioner, memiliki kontrol diri, pekerja keras, hingga menanamkan bentuk gotong royong. Namun, dengan kondisi keamanan dan pengawasan yang belum optimal terhadap data pribadi dari penggunanya, maka social network game justru dapat menjadi instrumen bagi pihak-pihak lain untuk melakukan operasi spionase dan mengumpulkan informasi intelijen yang kelak dapat mengancam keamanan nasional Indonesia di masa depan (Fuad, 2017). Dengan kondisi Indonesia yang saat ini menjadi pasar potensial bagi perkembangan social network game, peneliti tertarik untuk mengangkat tema ini sebagai fokus penelitian yang diharapkan dapat berkontribusi dalam perkembangan ilmu intelijen khususnya kajian intelijen siber dan information warfare.

Perkembangan teknologi dan informasi, telah mendorong meningkatnya penggunaan media sosial dalam berbagai komunikasi manusia. Hal ini telah membuka peluang bagi suatu negara untuk melakukan penyelidikan secara daring karena banyaknya informasi berguna yang terdapat pada di satu media yang bersifat digital. Misalnya, melalui pemeriksaan terhadap halaman profil dari akun media sosial seseorang. Informasi tersebut sering kali mencakup koneksi orang yang berkepentingan di platform tersebut. Termasuk di dalamnya berkenaan dengan pandangan politik, agama, etnis, negara asal, gambar dan video pribadi, nama pasangan (atau status perkawinan), alamat rumah dan kantor, lokasi yang sering dikunjungi, aktivitas sosial (misalnya, olahraga, teater, dan kunjungan restoran), riwayat pekerjaan, pendidikan, tanggal acara penting (seperti tanggal lahir, tanggal kelulusan, tanggal hubungan, atau tanggal meninggalkan/memulai pekerjaan baru), dan interaksi sosial yang mereka lakukan. Kondisi ini memungkinkan terjadinya spionase melalui platform digital yang berkaitan erat dengan aspek keamanan negara, mencakup teknologi, sumber daya manusia, maupun regulasi. Berdasarkan penjelasan tersebut, keamanan data dan spionase merupakan permasalahan strategis terkait keamanan dan kepentingan nasional. Oleh karena itu, penting melakukan kajian tentang ancaman spionase modern di era perkembangan teknologi yang pesat, khususnya spionasi melalui social network game di Indonesia.

Adanya potensi pencurian data melalui social network game oleh pihak asing yang dilakukan kepada pengguna di Indonesia melalui platform digital dapat membahayakan keamanan data pengguna dan dapat berdampak pada keamanan nasional. Oleh karena itu, penting untuk melakukan penelitian untuk mengidentifikasi potensi ancaman melalui aplikasi social network game di Indonesia. Tulisan ini bertujuan untuk menganalisis potensi ancaman yang ditimbulkan melalui aplikasi social network game di Indonesia.

1.1 Teori Ancaman

Irawan Sukarno (2014) menyebutkan bahwa ancaman merupakan kegiatan yang dapat merugikan, menimbulkan rasa sakit, mengganggu, menyulitkan dan membahayakan pihak lain. Sementara itu, John M. Collins menyebutkan terdapat tiga indikator dalam pengujian ancaman diantaranya adalah cara menilai celah keamanan, intensitas, dan kemampuan (Wahyono, 2003). Terdapat 5 sasaran dalam pelaksanaan ancaman, antara lain: (Fernando, 2019).

1) Negara, berkaitan dengan kepentingan ancaman terhadap kedaulatan negara;
2) Bangsa, berkaitan dengan kepentingan ancaman terhadap persatuan bangsa;

3) Pemerintah, berkaitan dengan kepentingan ancaman terhadap tindakan pemerintah;
4) Masyarakat, berkaitan dengan kepentingan ancaman terhadap kehidupan masyarakat;
5) Individu, berkaitan dengan kepentingan ancaman terhadap keamanan diri

1.2 Media Sosial

Media sosial didefinisikan sebagai segala bentuk media online yang memungkinkan komunikasi antar individu dan organisasi. Media sosial memungkinkan dialog antara perusahaan dan pelanggan melalui umpan berita dan profil media sosial yang berisi komentar, diskusi, dan jenis interaksi lainnya. Fondasi media sosial dapat ditelusuri kembali ke paradigma Web 2.0 yang berfokus pada konten yang dibuat pengguna dengan platform teknologi. Terdapat enam jenis platform media sosial menurut Andreas Kaplan dan Michael Haenlein (Fitriani, 2020):

1. *Collaborative projects*. Wikipedia termasuk ensiklopedia kolaboratif di mana semua orang bisa menulis, mengedit dan menambah isinya. Banyak orang menggunakan Wikipedia untuk menyelesaikan tugas dan pekerjaan rumah. Hanya saja yang perlu diingat, sesuai dengan sifatnya yang ‘kolaboratif,’ maka siapapun dapat menulis maupun mengubah informasi yang terdapat didalamnya. Untuk itu perlu klarifikasi mendalam setelah memperoleh informasi dari wadah ini.
2. *Content communities*. *Youtube* adalah sebuah situs web berbagi video (*video sharing*) yang populer dimana para pengguna dapat memuat, menonton, dan berbagi klip video secara gratis. Di *Youtube* kita dapat mengunggah video kita sendiri, mempromosikan video klip baru para musisi atau mempromosikan film – film baru.
3. *Blogs and microblogs*. Sekarang, *Twitter* menjadi salah satu media sosial yang paling banyak digunakan. Aplikasi yang sederhana hanya dengan meng-update status menjadi daya tarik para penggunanya.
4. *Social Networking Sites*. *Facebook* adalah sebuah layanan media sosial yang diluncurkan pada Februari 2004. Bermula dari jejaring sosial yang didirikan dan diperuntukan untuk mahasiswa Universitas Harvard, Amerika Serikat, kini *Facebook* menjadi media sosial paling popular di dunia. Di Facebook kita dapat berbagi atau *sharing* informasi, foto, dan video dengan teman dan keluarga.

5. *Virtual game worlds. Virtual Worlds* terikat berkaitan dengan *online gaming* dan *social networks, virtual world emulations* berubah dari eksperimental menjadi surga untuk *immersive communities.*
6. *Virtual social worlds*. *Second Life* merupakan dunia maya berbasis internet dan diluncurkan pada tahun 2003. Second Life merupakan suatu *platform* yang dikembangkan oleh perusahaan riset *Linden Research, Inc*. Komunitas maya ini menjadi perhatian dunia saat diliput oleh media berita pada akhir tahun 2006 dan awal 2007.

1.3 Konsep Network Society

Network Society merupakan sebuah konsep yang menggambarkan fenomena hubungan-hubungan antar manusia melalui berbagai media baru seperti hubungan antar manusia di dalam internet. Konsep *network society* merupakan konsep baru yang belum banyak diketahui oleh orang-orang. Konsep *network society* merupakan konsep baru dari perkembangan fenomena secara futurologi telah dijelaskan oleh Mc Luhan melalui konsep *global village electronic age*-nya. Fenomena yang terjadi di dalam *network society* memiliki kemiripan dengan fenomena yang terjadi dalam perkembangan ICT, sehingga konsep *network society* menjadi konsep yang lebih baru, bervariatif, dan berkembang (Surya, 2018).

Network society pertama kali dicetuskan melalui gagasan Mc Luhan yang perkembangan konsepnya ditandai dengan pemunculan konsep-konsep *information society* yang dijelaskan oleh Webster di tahun 1995. Konsep *network society* berisi berbagai penjelasan terkait dengan lima unsur utama komunikasi antar manusia. Lima unsur di dalam konsep *network society* sebagai berikut:

1. *Technological atau teknologi*
2. *Economic atau ekonomi*
3. *Accupational atau pekerjaan*
4. *Spatial atau spasial*
5. *Cultural atau budaya*

Konsep *network society* tidak hanya muncul dari perkembangan konsep *information society*. Konsep *network society* juga muncul dari penjelasan dan perkembangan konsep *The Wired Society, the post-industrial society.* Menurut James Marttin (dalam Surya, 2018) bahwa suatu kelompok masyarakat yang memiliki hubungan akan terhubung dengan jaringan telekomunikasi dan massa. Konsep *network society* juga dijelaskan oleh Barney (dalam Surya, 2018) yang mengartikan bahwa *network society* adalah konsep reproduksi dan

pelembagaan di seluruh dan di antara jaringan masyarakat tersebut sebagai bentuk dasar organisasi dan hubungan manusia di berbagai konfigurasi dan asosiasi sosial, politik, dan ekonomi. Konsep *network society* menurut Jan Van Dijk menjelaskan bahwa *network society* adalah konsep formasi sosial dengan infrastruktur jaringan sosial dan media yang memungkinkan mode organisasi utamanya di semua tingkatan (individu, kelompok/organisasi dan masyarakat).

Ide tentang konsep masyarakat informasi *network society* ini, sebenarnya pertama kali ditawarkan oleh Daniel Bell pada awal 1970-an melalui predisinya ketika itu tentang datangnya masyarakat pasca-industri *(post-industrial society)*. Pembahasan tentang masyarakat informasi ini kemudian dikembangkan lebih lanjut oleh Manuel Castells melalui konsep tentang masyarakat jaringan *(network society)*. Castell mengembangkan lebih lanjut konsep Daniel Bell, dan mengutarakan 4 pandangannya tentang kemunculan masyarakat, kultur dan ekonomi yang baru dari sudut pandang revolusi teknologi informasi, seperti televisi, komputer dan sebagainya (Surya, 2018).

Castells dalam mengkaji teorinya lebih fokus mengkaji peran perkembangan teknologi informasi dan informasi pada perkembangan jejaring perusahaan dan interaksi masyarakat. Castells sepakat dengan Beck melihat bahwa timbulnya risiko dari perubahan masyarakat ke era modernitas kontemporer, hanya saja Castells lebih melengkapi pemikiran Beck dengan dengan melihat lebih jauh peran teknologi informasi dan informasi. Dalam konteks network society, Castells menyatakan era itu yaitu masa transisi dari yang bersifat komunal menjadi individual. Dalam komunitas *cyberspace*, masing-masing individu memiliki peran yang jauh lebih besar melalui ikatan sosial yang terkadang melupakan ikatan fisik di antara mereka ke arah apa yang disebut Castells sebagai *me-centered networks*. Pada masyarakat informasional, Castells tidak secara khusus membahas terjadinya proses individualisasi yang melahirkan risiko yang makin besar di masyarakat, namun demikian ia mengakui bahwa di era masyarakat post-industrial telah terjadi perubahan dari kebudayaan massa dari industri kebudayaan yang terpecah-pecah. Dalam masyarakat informasional, struktur transnasional dan pergerakan sosial sebagai komunitas virtual, entitas global yang terdeteritorialisasi, yang ditopang oleh aliran-aliran penduduk, objek, dan tandatanda dari satu daerah ke daerah lain melalui televisi dan internet, dan juga bersandar pada kedatangan anggota-anggota mereka secara serentak ditempat-tempat tertentu (Surya, 2018).

2. METODOLOGI

Metode yang digunakan dalam penelitian ini adalah metode kualitatif. Metode ini didesain untuk mengungkapkan fenomena secara alamiah, analisis data bersifat induktif, dan peneliti sebagai instrumen utama dalam penelitian (Sugiyono, 2017). Desain kualitatif bersifat deskriptif, yaitu data dikumpulkan, dianalisis, dan dideskripsikan agar mudah dimengerti orang lain (Patilima, 2016). Penelitian ini menggunakan desain kualitatif deskriptif bertujuan untuk menganalisis potensi ancaman spionase melalui *social network game* di Indonesia dari perspektif intelijen. Metode kualitatif dapat membentuk interaksi langsung antara peneliti dengan informan agar mendapatkan data lengkap dalam penelitian (Moleong, 2013). Sumber data pada penelitian ini terbagi menjadi dua jenis yaitu, primer dan sekunder. Sumber data primer, yaitu Sumber data ini didapatkan langsung dari narasumber (Suyanto, 2008). Sumber data sekunder, yaitu Sumber data ini didapatkan dari studi literatur penelitian (Singarimbun, 2008).

Teknik analisis data kualitatif model Miles, Huberman, dan Saldana serta analisis intelijen digunakan dalam penelitian ini. Analisis intelijen digunakan untuk melihat dan memahami permasalahan berdasarkan sudut pandang intelijen. Jenis analisis ini dilakukan dengan memberikan *early detection* atau penilaian awal, membuat *forecasting* atau perkiraan di masa depan, merumuskan *early warning* atau peringatan dini, dan memberikan *problem solving* atau memberikan masukan sebagai solusi dari permasalahan penelitian (Sarosa, 2017). Teknik validasi yang digunakan adalah Triangulasi informan dan sumber data Triangulasi sumber adalah mengecek kredibilitas data melalui informasi yang didapatkan dari sumber sekunder (studi kepustakaan) dan sumber primer (informan). Triangulasi informan dilakukan dengan cara mengecek kredibilitas data melalui informasi yang didapatkan dari beberapa informan.

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Social Network Game di Indonesia

Social Network Game, dengan nama lain permainan yang dilakukan di media sosial, *game* sosial, *game* video sosial, atau *game* sosial daring, merupakan jenis permainan daring yang digunakan dan dimainkan melalui jejaring sosial, aplikasi media sosial, dan media sosial itu sendiri. *Social Network Game* adalah suatu bentuk permainan yang menampilkan mekanisme dan aturan permainan multipemain. Permainan multipemain merupakan suatu bentuk tipe permainan yang melibatkan banyak pengguna dan pemain dalam sebuah permainan media sosial. Permainan jejaring sosial awalnya diimplementasikan sebagai

permainan yang dapat diakses melalui *browser*. Namun, permainan jejaring sosial sekarang sudah bisa digunakan di dalam permainan seluler atau permainan *mobile*. Perkembangan teknologi yang terjadi di Indonesia menyebabkan perpindahan penyebaran dan penggunaan permainan sosial *browser* ke seluler. Pada era teknologi modern saat ini, masyarakat lebih banyak menggunakan permainan jejaring sosial seluler dibandingkan dengan permainan jejaring sosial di *browser*. Penggunaan permainan jejaring sosial di seluler lebih mudah diakses dan dapat dilakukan dimana saja dibandingkan dengan permainan jejaring sosial di *browser* atau komputer.

Perkembangan peminat permainan jejaring sosial semakin meningkat karena proses permainannya melibatkan kegiatan berbagi banyak aspek dari video permainan tradisional. Permainan jejaring sosial sering menggunakan aspek tambahan yang membuatnya berbeda. Secara tradisional, mereka berorientasi pada permainan sosial dan permainan kasual. Permainan jejaring sosial *"Facebook-to-Mobile"* adalah lintas platform pertama yang dikembangkan pada tahun 2011 oleh perusahaan Finlandia Star Arcade. Permainan jejaring sosial adalah salah satu permainan paling populer yang dimainkan di dunia, dengan beberapa produk dengan puluhan juta pemain. *Lil Green Patch, Happy Farm*, dan *Mob Wars* adalah beberapa permainan yang sukses pertama dari genre permainan global. *FarmVille, Mafia Wars, Kantai Collection*, dan *The Sims Social* adalah contoh terbaru dari permainan jaringan sosial yang populer di aplikasi penjualan permainan online global. Perusahaan besar yang membuat atau menerbitkan permainan jejaring sosial yang terkenal meliputi perusahaan *Zynga, Wooga*, dan *Bigpoint Games*.

Perkembangan sosial network game pada tahun 2010 dilaporkan bahwa secara demografi terdapat 55 persen permainan jejaring sosial di Amerika Serikat terdiri dari wanita. Sementara itu, di Inggris Raya, wanita merupakan hampir 60 persen. Selain itu, sebagian besar pelaku permainan aktivitas sosial berusia sekitar 30 hingga 59 tahun, dengan rata-rata *gamer* sosial berusia 43 tahun. Permainan sosial mungkin lebih menarik bagi demografi yang lebih tua karena gratis, lebih mudah untuk maju dalam waktu singkat, tidak melibatkan banyak kekerasan, seperti video permainan tradisional, dan lebih mudah dipahami oleh berbagai macam kalangan usia di dunia terkhusus masyarakat Indonesia. Permainan jejaring sosial lain menargetkan demografi tertentu yang menggunakan media sosial, seperti *Pot Farm* membuat komunitas dengan melibatkan unsur subkultur ganja dalam grafik dan tampilan *gameplay*-nya.

Permainan video jejaring sosial adalah aplikasi *client server* permainan sosial. Klien di era web diimplementasikan dengan campuran teknologi web seperti *Flash, HTML5, PHP,* dan *JavaScript*. Saat permainan *browser* sosial dipindahkan ke seluler, ujung depan permainan sosial dikembangkan menggunakan teknologi platform seluler seperti *Java, Objective-C,* dan *Swift*. Permainan jejaring sosial modern menggunakan banyak bahasa untuk melakukan aktivasi dan pemograman permainan tersebut. Istilah aktivasi atau pengaktivan pemograman tersebut memiliki sebutan yaitu *back-end. Back-end* adalah campuran dari bahasa pemrograman dan sistem termasuk PHP, Ruby, dan C++. Video permainan jaringan sosial menyimpang dari pengembangan permainan tradisional adalah kombinasi analitik *real-time*, untuk terus mengoptimalkan mekanisme permainan guna mendorong pertumbuhan, pendapatan, dan keterlibatan masyarakat di dalam pengguna permainan di media sosial.

Perubahan-perubahan teknologi yang terjadi di Indonesia dan perkembangan teknologi yang cukup pesat di Indonesia menyebabkan permainan video sosial menggunakan fitur-fitur baru dalam meningkatkan minat pengguna dan meningkatkan kualitas juga *display* permainan jejaring sosial tersebut. Fitur-fitur baru yang berkembang dalam perkembangan peningkatan kualitas permainan jejaring sosial meliputi sebagai berikut:

1. *Gameplay Ansikron*

Gameplay asinkron merupakan fitur permainan jejaring sosial yang memungkinkan aturan diselesaikan tanpa perlu pemain bermain pada saat yang bersamaan.

2. *Gameplay comunnity*

Gameplay community adalah fitur permainan jejaring sosial yang berkaitan dengan komunitas pengguna permainan jejaring sosial. Fitur ini merupakan fitur yang paling berbeda dari video permainan sosial karena fitur ini berhubungan dengan memanfaatkan jejaring sosial pemain. Misi atau tujuan permainan hanya dapat dilakukan jika pemain berbagi dengan teman yang terhubung melalui jejaring sosial yang menyelenggarakan permainan atau membuat mereka bermain. Semakin banyak kelompok masyarakat yang terhubung, semakin besar popularitas permainan tersebut dikenal oleh banyak orang di Indonesia.

3. *Gameplay Victory Conditions*

Gameplay victory conditions adalah kurangnya kondisi kemenangan dalam suatu konsep permainan. Fitur ini pada umumnya menjelaskan terkait dengan tidak adanya kondisi kemenangan karena sebagian besar pengembang permainan mengandalkan pengguna yang sering memainkan permainan mereka. Permainan tidak pernah berakhir

dan tidak ada yang pernah dinyatakan sebagai pemenang. Sebaliknya, banyak permainan kasual memiliki pencarian atau misi untuk diselesaikan pemain. Ini tidak berlaku untuk permainan sosial seperti permainan papan catur ataupun Scrabble di *browser*.

4. *Gameplay Virtual Currency*

Gameplay virtual currency adalah fitur yang menjelaskan mata uang virtual yang biasanya harus dibeli pemain dengan uang dunia nyata. Dengan mata uang dalam permainan, pemain dapat membeli peningkatan yang membutuhkan waktu lebih lama untuk diperoleh melalui pencapaian dalam permainan. Dalam banyak kasus, beberapa pemutakhiran hanya tersedia dengan mata uang virtual.

Fitur-fitur baru yang terdapat di dalam permainan ini menyebabkan adanya potensi ancaman spionase melalui social network game di Indonesia. Bentuk potensi ancaman itu dapat dilihat dari beberapa fitur-fitur baru yang penggunanya harus memasukan informasi pribadi pengguna tersebut. Informasi yang dimasukan di dalam permainan jejaring sosial tersebut tidak hanya meliputi informasi umum. Namun, informasi tersebut juga meliputi nomor kartu dan nomor rekening pribadi pengguna tersebut. Data pribadi yang digunakan untuk dapat bermain *game* ini merupakan data yang bersifat rahasia, sehingga jika data tersebut disalahgunakan akan mengakibatkan informasi rahasia milik pengguna berpotensi untuk disalahgunakan oleh orang-orang yang tidak bertanggung jawab. Dalam hal ini, faktor keamanan jaringan merupakan aspek penting bagi pengguna *game online*.

3.2 Potensi Ancaman Social Network Game di Indonesia

Bentuk ancaman spionase yang paling sederhana melalui *social network game* adalah ancaman ideologi kepada masyarakat. Hal ini dapat ditemukan melalui muatan konten seperti pornografi yang berdampak langsung kepada masyarakat khususnya pengguna *game*. Selain itu, ancaman yang ada juga dapat dilakukan melalui pencurian data pengguna melalui persetujuan pengguna ketika mengunduh aplikasi *game* tersebut. Ancaman tersebut juga dapat membahayakan keberadaan data individu di masing-masing aplikasi yang tertaut oleh akun pribadi pengguna *social network game* tersebut.

Bentuk ancaman pornografi yang berdampak langsung kepada masyarakat khususnya pengguna *game*. Dalam aplikasi *game*, terdapat permainan-permainan yang mengandung unsur pornografi. Globalisasi dan interkonektivitas *(interconnectivity)* melalui berbagai platform aplikasi teknologi informasi komunikasi membuat jangkauan berbagai muatan sosial (termasuk diantaranya data atau informasi) dapat menjadi potensi ancaman yang multi

dimensi, multi kompleks sehingga bentuknya pun menjadi beranekaragam, diantaranya *social network game*. Pengambilan informasi yang diambil oleh *social network game* pada dasarnya adalah informasi yang berkaitan dengan personal data seperti umur, *e-mail*, kontak nama, foto, lokasi atau *geo-location*, kartu kredit, data *facebook* dan lain sebagainya. Selain itu, bentuk ancaman spionase yang terjadi melalui *social network game* adalah banyaknya kasus pencurian data dan informasi pribadi yang terjadi karena pihak oposisi terus melakukan monitoring dan pengamatan berkaitan dengan data diri yang dimiliki oleh pengguna *social network game* tersebut. Semakin banyak akun yang login dengan aplikasi tersebut, semakin besar spionase tersebut akan terjadi.

Potensi ancaman dapat terjadi pada berbagai kegiatan melalui *social network game*. Potensi ancaman tersebut meliputi:

a. Penipuan online

Penipuan online melalui *social network game* dapat terjadi dalam berbagai bentuk, seperti penipuan *give away* palsu, penjualan item palsu atau modifikasi *game* yang dapat merusak perangkat pengguna. Penipuan semacam ini dapat merugikan pemain dengan cara mencuri data pribadi, uang, atau merusak perangkat pengguna.

b. *Cyberbullying*

Social network game dapat menjadi tempat untuk melakukan *cyberbullying*, terutama pada *game* yang memungkinkan interaksi antar pemain. Pengguna dapat menyebarkan ujaran kebencian, pelecehan, atau meminta uang dalam *game* secara paksa.

c. Konten yang tidak pantas

Beberapa *social network game* menyajikan konten yang tidak pantas seperti kekerasan, seks, atau bahasa kasar. Konten semacam ini dapat berdampak negatif pada pengguna, khususnya pada anak-anak yang masih rentan terhadap pengaruh lingkungan.

d. Serangan siber

Social network game dapat menjadi target serangan siber, seperti peretasan akun, pencurian data pribadi, atau *malware* yang menyerang perangkat pengguna.

e. Ketergantungan

Pengguna *social network game* dapat mengalami ketergantungan atau kecanduan pada permainan, sehingga berdampak pada kesehatan mental dan fisik mereka. Hal ini dapat memengaruhi kinerja sekolah, pekerjaan, dan hubungan sosial pengguna.

Dalam konteks *social network game*, kategorisasi potensi ancaman melalui *social network game* dapat terkait dengan upaya-upaya yang dilakukan oleh kelompok-kelompok ekstremis atau teroris untuk melakukan spionase atau memperoleh informasi rahasia yang dapat membahayakan keamanan nasional. Selain itu, ancaman juga dapat datang dari upaya-upaya subversi yang dilakukan oleh kelompok-kelompok yang ingin menggulingkan pemerintah atau merusak stabilitas politik di Indonesia.

Dalam hal ini, media sosial menjadi salah satu sarana yang dapat dimanfaatkan dalam menghadirkan berbagai bentuk potensi ancaman yang ditimbulkan melalui SNG.

Perkambangan revolusi industri 4.0 memungkinkan pelaku kejahatan mendapatkan informasi atau melakukan pencurian data melalui media sosial, salah satunya melalui *social network game*. Hal ini sejalan dengan konsep media sosial menurut Fitriani (2020) yang menjelaskan bahwa karakteristik khusus media sosial dan juga aplikasi *game online* mengarahkan para pencuri data untuk mengambil informasi. Kegiatan pencurian data melalui sosial media merupakan kegiatan spionase dalam bentuk yang modern di mana pelaku spionase dapat mengambil informasi dengan menggunakan teknologi canggih, seperti melalui *social network game* sehingga pengguna tidak menganggap tidak terjadi pencurian data.

Berdasarkan pada penjelasan di atas, terdapat delapan bentuk potensi ancaman melalui *social network game* di Indonesia. Delapan bentuk ancaman tersebut mencakup ancaman yang mempengaruhi ideologi masyarakat, pencurian data pengguna, penipuan *online, cyberbullying,* penyajian konten yang tidak pantas, serangan siber, efek ketergantungan kepada pengguna serta upaya-upaya subversi yang dilakukan oleh kelompok-kelompok yang ingin menggulingkan pemerintah atau merusak stabilitas. Merujuk pada jenis ancaman yang dijelaskan oleh Prunkcun (2019), maka potensi ancaman melalui *social network game* merupakan ancaman yang bersifat tak terlihat atau bersifat non konvensional. Dalam upaya mengatasi ancaman yang bersifat tak terlihat maka penting untuk membangun keamanan jaringan dalam upaya mengamankan informasi yang bersifat rahasia yang dimiliki oleh pengguna *social network game.*

Dalam konteks *social network game*, kategorisasi potensi ancaman melalui *social network game* dapat terkait dengan upaya-upaya yang dilakukan oleh kelompok-kelompok ekstremis atau teroris untuk melakukan spionase atau memperoleh informasi rahasia yang dapat membahayakan keamanan nasional. Selain itu, ancaman juga dapat

datang dari upaya-upaya subversi yang dilakukan oleh kelompok-kelompok yang ingin menggulingkan pemerintah atau merusak stabilitas politik di Indonesia. Dengan demikian, potensi ancaman spionase melalui *social network game* di Indonesia mencakup ancaman ideologi kepada masyarakat, pencurian data pengguna, ancaman pornografi, penipuan online, *cyberbullying* dan ketergantungan. Hal ini menunjukkan bahwa potensi ancaman spionase melalui *social network game* di Indonesia dilakukan oleh individu atau kelompok yang bertujuan untuk menimbulkan ancaman secara nyata ataupun tidak nyata kepada penggunanya.

Hal ini sejalan dengan penjelasan yang dikemukakan oleh Iwan (2012) bahwa ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat yang dapat menimbulkan berbagai ancaman fisik, baik nyata ataupun yang tidak nyata dengan menggunakan kode-kode komputer *(software)* atau perangkat keras *(hardware)* untuk melakukan gangguan terhadap sistem *(network instruction)* ataupun penyebaran. Selain itu, hal ini juga sejalan dengan hasil penelitian yang dijelaskan Cathy Downes (2018) *Strategic Blind Spots on Cyber Threats, Vectors and Campaigns* bahwa perkembangan *machine learning* yang merupakan bagian dari teknologi persuasif telah merubah tren dalam domain peperangan siber ke arah pemrograman manusia (persepsi). Perusahaan analitik data yang memanfaatkan data dari pengguna akan dapat dipergunakan sebagai modal dari operasi intelijen suatu negara yang dapat diasumsikan termasuk kegiatan spionase siber.

Dengan memperhatikan hasil penelitian yang menunjukan delapan bentuk potensi ancaman melalui *social network game* di Indonesia maka merujuk pada konsep ancaman yang dikemukakan oleh Soegirman, potensi ancaman melaui *social network game* di Indonesia dikategorikan sebagai potensi ancaman kritis. Kategori ini merujuk pada definisi Soegirman bahwa suatu ancaman dikategorikan kritis apabila ancaman tersebut merupakan ancaman yang menyangkut eksistensi, integrasi, dan kedaulatan NKRI. Apabila potensi ancaman tersebut tidak ditangani dengan serius oleh pihak-pihak yang berkompeten maka dapat menjadi ancaman yang dapat mengganggu eksistensi, integrasi serta kedaulatan negara. Hal ini dilatarbelakangi oleh bentuk-bentuk potensi ancaman spionase yang berkaitan dengan unsur-unsur vital di dalam masyarakat seperti ideologi dan juga data diri pengguna, dalam hal ini adalah masyarakat.

Dalam upaya melindungi informasi pengguna *social network game* secara khusus dan pengguna media sosial secara umum, maka Pemerintah, dalam hal ini Kemenkominfo, BSSN dan BIN sebagai Lembaga perlu untuk membentuk lingkungan digital yang aman. Hal ini sebagaimana dijelaskan oleh Presiden Joko Widodo dalam pembukaan KTT G20 di Bali bahwa terdapat tiga hal yang menjadi perhatian untuk meningkatkan transformasi digital, yaitu: adanya kesetaraan akses digital, literasi digital dan mewujudkan lingkungan digitan yang aman. Dalam memperkuat pernyataan tersebut, Kepala Badan Siber dan Sandi Negara (BSSN), dalam buku Annual Report BSSN Tahun 2022 menyatakan bahwa dalam mewujudkan lingkungan digital yang aman, BSSN telah menyusun berbagai program keamanan siber. Hal ini dilakukan dalam upaya adaptif dan inovatif dalam rangka melindungi seluruh lapisan ruang siber, termasuk asset informasi yang berada dalam ruang siber/digital dari berbagai hakikat ancaman dan serangan siber. Dalam upaya mewujudkan semua ini, koordinasi dan kolaborasi sebagai elemen utama dalam sinergi merupakan aspek penting dalam membangun keamanan siber karena mewujudkan keamanan siber merupakan tanggung jawab seluruh stakeholders pada ranah siber yang dikoordinasikan oleh BSSN.

4. KESIMPULAN

Potensi ancaman melalui social network game di Indonesia adalah ancaman yang dapat mengancam pengguna social network game di Indonesia. Potensi ancaman tersebut meliputi ancaman ideologi di masyarakat, konten ilegal dan pornografi semakin berkembang, pencurian data diri, monitoring aktivitas pengguna secara ilegal, penipuan online, cyberbullying, konten-konten yang tidak pantas, ketergantungan, dan serangan cyber yang mengancam aktivitas pengguna social network game di Indonesia. Ancaman tersebut dapat berkembang dengan cepat karena pengguna social network game di Indonesia semakin banyak dan populer.

Penelitian ini memiliki keterbatasan, sehingga perlu penelitian lebih lanjut untuk mengkaji secara mendalam terkait berbagai potensi ancaman spionase melalui social network game di Indonesia terutama pada aspek pencurian data, konten-konten ilegal, dan pornografi di social network game serta memperdalam permasalahan terkait dengan strategi intelijen dalam menghadapi ancaman spionase melalui social network game di Indonesia terkhusus pada aspek sarana, cara, dan tujuan strategi tersebut dalam mengatasi ancaman spionase.

Dalam upaya mengatasi berbagai potensi ancaman tersebut, pemerintah perlu bekerja sama dengan pakar teknologi dan siber yang ada di Indonesia, serta berbagai media sosial untuk melakukan tindakan monitoring, filtering, juga pembatasan terhadap berbagai social network game yang tingkat keamanannya masih rentan—sehingga dapat membahayakan para pengguna dalam menjalankan aplikasinya tersebut. Pemerintah disarankan perlu meningkatkan monitoring dan pendalaman terkait ancaman melalui social network game di Indonesia secara teknis, taktik, prosedur, dan strategi yang dilakukan oleh para pakar siber dan juga melalui keahlian para hacker. Hal itu dapat membantu menentukan strategi intelijen yang tepat dalam menghadapi berbagai ancaman yang mungkin timbul.

6. DAFTAR PUSTAKA

Barclay, D. A. (2018). *Fake News, Propaganda, and Plain Old Lies: How to Find Trustworthy Information in the Digital Age.* Maryland: Rowman & Littlefield.

Fernando, Y. (2019). Identifikasi Ancaman PCI (Positif Clandestine Intelligence) Berbentuk Cyber Terrorism Terhadap Keamanan Nasional. *Jurnal Kajian Stratejik Ketahanan Nasional, 2 (1)*, 31-40.

Fitriani, Y. &. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *Jurnal Humaniora*, 2579-3314. Retrieved from http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala

Fuad, Z. A., & Helminsah. (2017). *The Impact of Online Games on Social and Cognitive Development on Elementary School Student, Proceedings of the 1st International Conference on Innovative Pedagogy* . Banda Aceh: ICIP.

Ivanjko, T. (2019). *Open Source Intelligence (OSINT): Issues and Trends, INFuture.* Knowledge in the Digital AgeIINFuture2019.

Iwan, D. (2012). *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber.* Jakarta: Tesis Universitas Pertahanan Indonesia.

Krishnamurthy. (2009). On the leakage of personally identifiable information via online social networks. *In: Journal and Proceedings of the 2nd ACM workshop on Online social networks*, 7-12.

Moleong, L. J. (2013). *Metode Penelitian Kualitatif.* Bandung: PT. Remaja Rosdakarya.

Narayanan, A. (2010). Myths and fallacies of" personally identifiable information". *Journal Communications of the ACM, 53 (6)*, 24-26.

Patilima, H. (2016). *Metode Penelitian Kualitatif.* Bandung: Alfabeta.

Sarosa, S. (2017). *Penelitian Kualitatif Dasar-Dasar.* Jakarta: PT Indeks.

Schwartz, P. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *Journal of NYUL Revition, 86*, 1814.

Shoelhi, M. (2012). *Propaganda dalam Komunikasi Internasional.* Bandung: Simbiosa Rekatama Media.

Singarimbun, M. (2008). *Metode dan Proses Penelitian.* Jakarta: LP3ES.

Sugiyono. (2017). *Metode Penelitian Kuantitatif.* Bandung: Alfabeta.

Sukarno, I. (2011). *Aku "Tiada" Aku Niscaya: Menyingkap Lapis Kabut Intelijen.* Jakarta: Yayasan Pustaka Obor Indonesia.

Sukarno, I. (2014). *Ilmu Intelijen.* Sentul: STIN Press.

Surya, S. (2018). "Informasionalisme, Network Society, dan Perkembangan Kapitalisme: Perspektif Manuel Castells. *Journal Sistem Pelayanan Informasi dan Kehumasan Pemerintah*, 1-12.

Suyanto. (2008). *Metode Penelitian Sosial: Berbagai Alternatif Pendekatan.* Jakarta: Kencana.

Wahyono. (2003). Pengertian dan Lingkup Keamanan Nasional. *Jurnal Kajian Stratejik Ketahanan Nasional, 1*, 19-20.

Walters, V. (1978). *Silent Missions.* New York: Garden City.

Wati, V. O. (2021). Indonesia's Foreign Policy in Pacific Island Countries during Joko Widodo Era 2014-2019: An Adaptive Action? *Journal of Global Strategis, 15 (1)* , 1-24