Aisyah Journal of Informatics and Electrical Engineering
Universitas Aisyah Pringsewu

Journal Homepage
http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Cyber Security and The Challenge of Society 5.0 Era in Indonesia

Dita Septasari

Magister Teknik Informatika, Fakultas Ilmu Komputer
Intitut Informatika dan Bisnis Darmajaya
ditaseptasari.2221210069@mail.darmajaya.ac.id

ABSTRACT

Information security becomes crucial in the era of Society 5.0. The era of Society 5.0, where every aspect of human life relies on the use of information and communication technology. Almost all things in life, especially in human interactions, relies on the internet and information technology devices. Era Society 5.0 facilitating human life with the help of various technological advancements such as IoT (Internet Of Things) and AI (Artificial Intelligence). The convenience provided by Era Society 5.0 also has challenges that attack cyberspace. Cyberattacks can attack individuals and the integrity of nations and countries. Cyber attacks must be handled appropriately in accordance with applicable law in Indonesia. Indonesia is the countries whose cyber security is still weak, so it is necessary to cooperate with all parties in strengthening cyber security in Indonesia, including by enacting the ITE Law which strengthens cyber security in Indonesia.

Keywords: *Cyber Security; Cyber Crime; Era Society 5.0; Indonesia*

ABSTRAK

Keamanan informasi menjadi salah satu aspek krusial dalam era Society 5.0. Seiring memasuki era Society 5.0, di mana setiap aspek kehidupan manusia bergantung pada penggunaan teknologi informasi dan komunikasi. Hampir seluruh aspek kehidupan, terutama dalam interaksi antar manusia, memanfaatkan internet dan perangkat teknologi informasi. Era *Society* 5.0 mempermudah kehidupan manusia dibantu dengan berbagai kemajuan teknologi seperti IoT (*Internet Of Things*) dan AI (*Artificial Intelligence*). Kemudahan yang diberika oleh Era *Society* 5.0 juga terdapat tantangan yang menyerang dunia *cyber*. *Cyber attack* bisa menyerang individu perseorangan dan integritas bangsa dan negara. Serangan *Cyber* harus ditangani dengat tepat sesuai hukum yang berlaku di Indonesia. Indonesia merupakan negara dengan *cyber security* yang masih lemah, sehingga perlu kerjasama semua pihak dalam memperkuat cyber security di Indonesia, termasuk pembuatan Undang-Undang ITE yang memperkuat *cyber security* di Indonesia.

Kata Kunci: *Cyber Security; Cyber Crime; Era Society 5.0; Indonesia*

I. PENDAHULUAN

Keamanan sistem informasi pada era scociety 5.0 menjadi faktor yang sangat signifikan dalam perkembangan teknologi informasi. Era *Society* 5.0 bertujuan untuk meningkatkan kuliatas hidup masyarakat dengan mobilisasi potensi produktif dan meberikan kenyamana dalam kehidupan manusia dalam pemanfaatan teknologi seperti *Internet Of Things* (IoT), *Artificial Intelligence* (AI) atau Robot. [1] Penggunaan internet yang dilakukan hampir seluruh sektor kehidupan manusia, baik dalam bidang industri, teknologi, *marketing*, hingga sampai ke aspek pendidikan. Terutama semenjak pandemi Covid-19 semua aspek kehidupan meminimalisir interaksi antarmanusia dan menjadikan teknologi menjadi tangan untuk menghubungkan segala aspek kehidupan manusia. Pasca pandemi Covid-19 perkembangan data dan teknologi yang digunakan mencangkup seluruh aspek, keamanan informasi pengguna menjadi hal yang sangat penting saat ini. Perkembangan teknologi informasi juga mengubah cara hidup manusia. Sebelumnya, masyarakat cenderung berfokus pada lingkungan lokal, namun saat ini mereka beralih ke kehidupan yang bersifat global, di mana segala hal dapat dilakukan dalam dunia maya.. [1]

Perkembangan keilmuan keamanan informasi dalam era society 5.0 memiliki resiko dalam dunia cyber bisa mencangkup kerahasiaan atapun Integritas baik organisasi ataupun perseorangan. Kejahatan saat ini bukan hanya seara langsung seperti perampokan pencurian atau lainnya, kejahatan saat ini dapat berkembang dalam dunia maya yang biasa disebut dengan *cyber crime*. Tindak kejahatan yang relatif baru ini dilakukan oleh orang-orang yang memiliki keahlian dibidang kompter dan teknologi informasi. Komputer yang sebelumnya digunakan sebagai alat untuk mempermudah pengumpulan dan penyimpanan informasi serta pekerjaan, saat ini dapat dimanfaatkan oleh individu yang tidak bertanggung jawab untuk melakukan tindakan kejahatan. [2] *Cyber security* bertujuan untuk melindungi jaringan, perangkat maupun program dari berbagai ancama cyber dan akses ilegal terhadap data-data pengguna. Berdasarkan data sistem monitoring traffic ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*) serangan di dalam dunia maya Indonesia mencapai satu juta insiden dan mengalami peningkatan setiap harinya akibat kelemahan sistem yang tidak atau belum diketahui. Dalam 1998-2009 sebayak 2.138 telah mencoba untuk menyerang sistem domain pemerintahan. [2].

Serangan *Cyber* atau *Cyber Crime* di Indonesia menyerang berbagai jenis platform baik jejaring media sosial seperti facebook, twitter, instagram atau media masa yang banyak diakses oleh banyak orang dan menggandung informasi pribadi. Pada beberapa kesempatan, sebagai pengguna, terdapat banyak informasi pribadi yang seharusnya tidak sebarluaskan secara global dan dapat disalahgunakan oleh individu yang tidak bertanggung jawab, dengan tujuan untuk mengambil informasi pribadi pengguna. Pengguna yang bijak dapat mengurangi kehatan dalam dunia cyber. Dalam penelitian "Pengenalan *Cyber Security* Sebagai Fundamental Keamanan Data Pada Era Digital" menyebutkan isu yang muncul dalam dunia cyber dalam segala aspek kehidupan seperti politik, militer, ekonomi, sosial dan budaya seperti *cyber terrorism, cyber crime* dan *cyber war*.[2]

II. TINJAUAN PUSTAKA

A. *Cyber Crime*

Cyber Crime merupakan kajahatan yang dilakukan di internet yang memanfaatkan kemajuan infrastruktur Teknologi Informasi dan Komunikasi. Kasus *cyber crime* sudah sering terjadi di Indonesia dibuktikan dengan 4.586 laporan yang dicatat oleh Direktori Tindak Pidana Siber Bareskrim Polri dari Januari sampai Desember 2019. Denagn 1.617 kasus atau kebanyakan merupakan laporan penipuan online yang merucut kepada *e-commerce* yaitu pembelian atau penjualan secara online.[3] Pandemi Covid-19 yang terjadi beberapa tahun yang lalu dapat menyebabkan kemiskinan dan mengakibatkan kemungkinan meningkatnya tindakan kejahatan baik dalam dunia nyata atau dunia *cyber*. Kejahatan di dunia *cyber* harus ditangani dengan tepat untuk keselamatan pribadi atau negara, tanpa upaya *cyber security* yang tepat kejahatan di dunia *cyber* akan semakin meningkat.[4]

B. *Cyber Security*

Cyber security adalah suatu mekanisme atau kebijakan yang bertujuan untuk melindungi dan

mengamankan sumber daya digital, melalui penggunaan pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi, yang digunakan untuk melindungi sistem dan aset pengguna dari ancaman cyber. *Cybersecurity* meliputi perlindungan terhadap infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan informasi yang disimpan dalam lingkungan maya atau *cloud*. *Keamanan siber* memastikan bahwa pemeliharaan mencakup perlindungan organisasi atau aset pengguna [5]

Dalam beberapa tahun terakhir, kemajuan dan perkembangan teknologi informasi dan komunikasi telah memberikan dampak positif pada kemajuan ekonomi, baik dalam skala lokal maupun global. Selain itu, perkembangan teknologi informasi juga memberikan dampak pada peningkatan produktivitas, meningkatnya persaingan, dan keterlibatan warga dalam kebijakan pemerintahan yang lebih tinggiHal ini memiliki konsekuensi bagi pemerintahan, pengusaha, dan masyarakat yang semakin mengandalkan lingkungan digital atau dunia maya. Beberapa tantangan di lingkungan digital memerlukan perhatian yang lebih besar terhadap penguatan keamanan siber atau keamanan cyber yang lebih kuat. *Cybersecurity* memastikan perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi di *cyberspase*. *Cyberspase* sendiri merupakan lingkungan hasil dari interaksi antar peraangkat lunak, orang-orang dan layanan internet dengan menggunakan berbagai perangkat teknologi informasi dan koneksi jaringan uang tidak memiliki wujud.[4]

Cyber Security merupakan jenis kejahatan baru yang menyerang pada dunia maya yang bisa menyerang siapapun kapanpun dan dimanapun. *Cyber crime* dapat menyerang sampai ketahap integritas negara bukan hanya perorangan. Semakin meningkatanya penggunaan teknologi informasi sejalan dengan semakin meningkatnya tindakan kejahatan di dunia *cyber*. *Cyber Security* dalam praktiknya melindungi perangkat komputer, mobile sever dan sistem elektronik ataupun jaringan dari serangan-serangan digital. *Cyber Security* semakin populer sejalan dengans semakin bannyaknya penggunaan teknologi informasi dan komunikasi seperti laptop, dekstop, perangkat *Internet Of Things* (IoT), smartphone, server, serta jaringan internet dalam kehidupan sehari hari. [4]

C. Era *Society* 5.0

Era Society 5.0 mencerminkan perubahan yang signifikan dalam tatanan kehidupan dan cara kerja manusia. Pada era ini kemajuan teknologi informasi dan komunikasi telah menghubungkan antara dunia fisik dan dunia maya, atau dunia siber. Era *Society* 5.0 membuat fase baru dalam kemajuan teknologi informasi yang memungkinkan kita menggunakan ilmu pengetahuan yang berbasis IoT (*Internet Of Things*), *Atrificial Intellegence* dalam kehidupan manusia dengan tujuan membuat kehidupan manusia lebih nyaman.

III. METODOLOGI

Pada jurnal ini membahas tentang keberadaan *cyber security* yang terus berkembang sejalan dengan perkembangan teknologi dan tantangannya di era *Society* 5.0. Era *Society* 5.0 menawarkan masyarakat yang berfokus pada manusia dengan menciptakan keseimbangan antara kemajuan ekonomi dan penyelesaian masalah sosial melalui sistem yang menghubungkan dunia maya dan dunia nyata. Metode yang diterapkan dalam penelitian ini merupakan metode deskriptif kualitatif. Metode kuantitatif deskriptif adalah suatu pendekatan penelitian yang menjelaskan prosedur penelitian yang menghasilkan data dalam bentuk angka atau tulisan yang mewakili objek yang diamati.[6] Pada penelitian ini bertujuan untuk mendeskripsikan tentang kemananan cyber dan tantangannya pada Era *Society* 5.0.

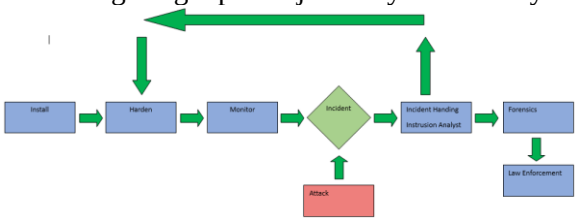
IV. HASIL DAN PEMBAHASAN

A. *CYBER SECURITY* di Indonesia

Keamanan siber adalah isu yang relatif baru dan muncul ketika semua aspek kehidupan, termasuk ekonomi, sosial, budaya, politik, dan militer, terhubung dengan dunia maya. [2] Beberapa kejadian belakangan ini memasukkan Indonesia kedalam negera yang memiliki *Cyber Security* yang masih lemah. Hal ini dibuktikan dengan beberapa kejadian seperti peretasan terhadap data pengguna atau nasabah Bank yang baru-baru ini terjadi karena *ransomeware*. *Ransomware* merupakan serangan kriminal yang mengincar perangkat lunak dengan tujuan membatasi akses pengguna terhadap file, mengunci layar pengguna, atau mengenkripsi file, dan pada akhirnya meminta tebusan.[7]

Selain ransomeware ancaman dalam dunia *cyber* dapat berupa *cyber terrorism*, *cyber crime* dan *cyber war*. Indonesia merupakan negara dengan populasi terbesar di kawasan Asia Tenggara dengan 277,43 Juta jiwa pada tahun 2023, hal ini tidak terlepas dari ancaman-ancaman *cyber attack* tersebut.

Ruang Lingkup Kebijakan Cyber Security



Sumber : *Technology Perscpetive: National Cyber-Security, Universitas Pertahanan Indonesia*

Ruang lingkup keamanan siber dimulai dengan *Intsall* dan kemudian *herden* yakni penguatan keamanan terkait dengan perangkat keras yang digunakan dalam operasionalisasi monitor dan internet. Hal ini bertujuan untuk mencegah terjadinya insiden atau kejadian yang disebabkan oleh serangan siber atau serangan *cyber*, yang kemudian dapat ditangani melalui uji forensik sebagai bukti dalam penegakan hukum terhadap *cyber crime*.

Tujuan utama dari *cyber security* adalah untuk mengurangi risiko dan melindungi kerahasiaan, integritas, dan ketersediaan informasi dari berbagai gangguan.

Elemen-elemen dalam *cyber security* meliputi :

1. Dokumen kebijakan keamanan (*security policy*) adalah dokumen yang digunakan dalam pelaksanaan berbagai proses yang terkait dengan keamanan informasi.
2. Infrastruktur Teknologi Informasi yang merupakan perangkat *hardware* dan *software* sistem operasi.
3. Penilaian keamanan jaringan adalah elemen yang bertindak sebagai mekanisme kontrol yang memberikan pengukuran terhadap tingkat keamanan informasi.
4. *Perimeter Defense* adalah sarana yang berperan penting dalam pertahanan infrastruktur informasi, seperti IDS (Sistem Deteksi Intrusi), IPS (Sistem Pencegahan Intrusi), dan firewall.
5. Sistem Informasi dan *Event Management* adalah alat yang berfungsi untuk memantau berbagai kejadian jaringan yang terkait dengan insiden keamanan.
6. Sistem Monitoring Jaringan merupakan media yang berperan dalam monitoring utilitas, kelayakan atau performa infrastruktur informasi.
7. Sumber Daya Manusia dan kesadaran tentang keamanan informasi pengguna.

Keamanan Teknologi Informasi bukan hanya tentang keamanan *cyber* tetapi juga bisa berupa *physical security* termasuk di dalamnya data center, sistem pemulihan jika terdapat kejadian *cyber attack* dan media transmisi. [5]

B. TANTANGAN DI ERA *SOCIETY* 5.0 DI INDONESIA

Dalam era *society* 5.0 dalam perkembangannya terdapat tantangan-tantangan yang dihadapi seperti keterampilan dalam penggunaan teknologi, kejahatan pada dunia *cyber* yang menyerang bukan hanya perorangan tetapi juga kejahatan *cyber* yang menyerang integritas dan kredibilitas organisasi atau negara. Saat ini setiap pekerjaan baik perorangan atau organisasi mengunakan teknologi yang menghubungkan ke dunia maya. Data publik maupun data pribadi dapat diakses oleh siapapun kapanpun dan dimanapun. Semua ini tergantung kepada bagaimana setiap individu mampu mengelola dan mem-*privacy* data pribadi masing-masing. [6].

Konsep Era *Society* 5.0 pertama kali diperkenalkan oleh Jepang. Era Society 5.0 bertujuan untuk menciptakan masyarakat super pintar (*super smart society*, SSS), di mana teknologi informasi menjadi kebutuhan penting bagi seluruh masyarakat. Era *society* 5.0 menghadapi berbagai tantangan seperti *cyber attack* atau ancaman di dunia digital yang mengancam berbagai keamanan seperti :

1. Ancaman dalam ranah sosial dan budaya meliputi pelanggaran hak cipta, pencurian identitas, serta penyebaran konten pornografi berupa foto atau video.
2. Ancaman Teknologi, seperti melakukan *pishing* atau penipuan atau pengelabuhan pengguna sistem, serangan *cyber* DDoS (*Distributed Denial Of Service*), melakukan akses ke situs-situs ilegal, dan memanfaatkan *dark web* untuk kegiatan atau aktivitas ilegal yang merugikan perseorangan atau berbagai pihak.
3. Ancaman Ekonomi, seperti penipuan yang dilakukan secara online dalam sektor

finansial seperti penipuan dari jual beli yang ada di dalam *e-comerce i* dan kejahatan dalam *e-commerce* merupakan kejahatan yang paling sering terjadi karena paling dekat dengan masyarakat.

4. Ancaman ideologi, seperti mudahnya penyebaran ajaran radikal dan terorisme melalui internet yang bisa diakses oleh berbagai kalangan baik dewasa atau remaja, dalam hal ini kalangan remaja merupakan target yang mudah untuk di berikan informasi-informasi terhadap kesalahan pemahaman ideologi dan mengakibatkan terjerumusnya kapada ajaran-ajaran sesat dan tidak sesuai dengan kaidah atau ajaran agama.
5. Ancaman terhadap keamanan publik melibatkan serangan *cyber* yang ditujukan pada infrastruktur informasi nasional yang kritikal.
6. Ancaman politik, seperti maraknya serangan provokasi politik, anti pemerintahan, SARA dan hoax yang bisa menyebar dengan cepat dengan bantuan beberapa orang yang mudah percaya terhadap berbagai informasi tanpa melakukan *crosscheck* terhadap informasi yang beredar. Dalam hal ini informasi berbau sara, politik, anti pemerintah atau hoax dengan mudah bisa melakui grup-grup *chatting* atau sosial media yang bisa diakses kapanpun dan dimanapun.

Tantangan yang di hadapi di Era *Society* 5.0 merupakan ancaman yang bisa mengancam keselamatan pribadi perseoranagan, organisasi, atau integritas bangsa dan negara. Pengguna yang bijak harus berhati-hati dalam menggunakan teknologi terutama generasi milenial yang merupakan *Agent Of Change* atau Agen Perubahan. Generasi milenial dengan kelahiran 1980-1995 merupakan generasi yang paling banyak menggunakan akses teknologi informasi baik untuk bekerja, sosial media, email, web *chatting* atau lainnya. Keadaan saat ini terdapat berbagai kecanggihan Teknologi informasi yang dapat dimanfaatkan oleh generasi milenial. Generasi milenial memiliki peran dan tantangan penting sebagai generasi perubahan yang diharapakan dapat menghadirkan berbagai inovasi teknologi terbarukan yang bisa bermanfaatkan bagi bangsa dan negara.[8]

C. KEBIJAKAN DAN HUKUM *CYBER* DI INDONESIA

Dalam menangani masalah hukum dalam ranah siber, diperlukan keberadaan undang-undang yang dikenal sebagai hukum siber atau *Cyber Law*. *Cyber Law* merupakan bidang hukum yang berakar dari *Cyberspace Law*, yang mencakup berbagai aspek yang terkait dengan individu atau entitas hukum yang memanfaatkan teknologi internet atau elektronik. Semua kegiatan yang dilakukan secara daring atau melalui internet telah menjadi bagian dari dunia siber.

Dunia *Cyber* dibagi menjadi beberapa hal :

1. Hak merek (*Trademark*)
2. Penistaan, fitnah dan penghinaan (*hate speech*)
3. Penyerangan terhadap komputer termasuk perangkatnya (*Hacking, Viruses, Illegal Access*)
4. Kenyamanan Pribadi (*Privacy*)
5. Kejahatan dengan memanfaatkan Teknologi Informasi (*Criminal Liability*)
6. Pencemaran nama baik (*Defamation*)
7. Transaksi Elektronik (*Electronic Contract*)
8. Pornografi
9. Hak Cipta (*Copy Right*)
10. Pengaturan sumber daya internet (*Regulation Internet of Resource*)
11. Pencurian melalui Internet (*Robbery*)
12. Perlindungan Konsumen (*Customer Protection*)
13. Penyelidikan, pembuktikan, dll (*Procedural Issue*)
14. Pemanfaat internet untuk kejahatan dalam ruang lingkup *E-Commerce* atau *E-Government*

Cyber Law sangat dibutuhkan sebagai dasar hukum dalam menangani tindakan kejahatan dalam dunia *cyber* seperti pencurian data atau penipuan. Segala tindakan kejahatan dalam dunia *cyber* Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan dari Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam hal ini UU ITE merupakan langkah pencegahan terhadap tindak pidana dan merupakan dasar hukum untuk menangani kejahatan yang terjadi melalui komputer dan sarana elektronik lainnya. Kejahatan *cyber* merupakan kejahatan transional maka menggunakan hukum nasional tetapi jika terdapat kejahatan *cyber* yang tidak tercantum pada hukum nasional, maka prinsip-prinsip hukum internasional digunakan sebagai

acuan atau pedoman.. Undang-Undang Nomor 19 Tahun 2016 diharapkan menjadi kekuatan dalam pengendalian dan penegakan ketertiban dalam setiap kegiatan yang memanfaatkan teknologi informasi baik dalam segala hal yang berkaitan dengan internet maupun dalam memanfaatkan perangkat komputer dan alat elektronik lainnya.[9]

D. STRATEGI PENGUATAN *CYBER SECURITY* DI INDONESIA

1. Peningkatan kemampuan Pengetahuan *Cyber*

Sebagai pengguna yang berada dalam *cyberspace* penting untuk meningkatkan kemampuan pengetahuan tentang pentingnya *cyber security*. Langkah pengingkatan pengetahuan tentang *cyber security* bertujuan sebagai langkap pencegaahan dalam menghadapi *cyber crime*. Menghadapi *cyber crime* merupakan keharusan bagi setiap individu dan pemerintah yang segala aktifitas kehidupan menggunakan teknologi informasi dan tentunya perlu kerjasama semua pihak baik pemerintah maupun individu/masyarakat. Pemerintah membangun komunitas keamanan *cyber* dengan tujuan mencegah, melawan, dan mendeteksi potensi serangan *cyber* secepat mungkin, dengan maksud untuk memperkuat ketahanan dan keamanan nasional serta melindungi warganegara.[4]

2. Penguatan Undang – Undang Tindak Pidana *Cyber* di Indonesia

Undang-Undang Nomor 8 Tahun 2011 yang saat ini diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Traknsaksi Elektronik (UU ITE) yang mengatur segala transaksi ataupun pelanggaran yang terjadi dalam penggunaan Teknologi Informasi menjadi penguat terhadap segala tindakan yang dilakukan dalam penggunaan teknologi informasi di Indonesia termasuk dokumen elektronik, sistem elektronik, penyelenggara sistem elektronik, jaringan dan agen elektronik, tanda tangan dan sertifikat elektronik, perangkat keras ataupun perangkat lunak komputer dan lain lain termasuk ke dalam UU ITE. Peran pemerintah dan semua pihak termasuk masyarakat terhadap keamanan cyber menjadi penguat bagi undang-undang yang sudah dibuat di Indonesia. Selain Undang-undang dan langkah preventif dari setiap masyarakat terdapat peran penting keilmuan IT yang membantu dalam mengintegrasikan dalam strategi penguatan *cyber security* di Indonesia, yaitu :

a. Pengembangan sistem informasi sesuai dengan perkembangan jaman. Perkembang sistem informasi yang responsif terhadap tren dan perkembangan serangan/*cyber attack* dan ancaman keamanan informasi.
b. Pengembangan sumber daya manusia (SDM).Peningkatan kualitas sumber daya manusia (SDM) melalui kesadaran akan pentingnya privasi dan keamanan siber.
c. Turut dalam kampanye *Agent of Change*/Agen Perubahan. Agent of Change bagi generasi millenial tentang kesadaran dan pentingnya menggunakan teknologi yang positif di tengah mudahnya dalam mengakses konten-konten negatif mengguanakan teknologi informasi di Era *Society* 5.0.[10]

V. PENUTUP

A. Kesimpulan

Keamanan *cyber* manjadi hal yang penting seiring dengan kemajuan teknologi informasi yang pesat. Dalam dunia *cyber* terdapat kekurangan dan kelebihan dalam penggunaannya. Di indonesia terdapat peraturan perundang-undangan yang mengatur penggunaan teknologi informasi dan komunikasi di Indonesia dan dalam perkembangannya masih terdapat banyak serangan atau kejahatan yang menyerang *cyber* Indonesia. Perlu adanya kerjasama berbagai pihak baik dari pemerintah dan masyarakat yang secara langsung menggunakan teknologi informasi, selain itu setiap warga negara wajib bertangung jawab terhadap teknologi informasi yang digunakan.

B. Saran

Saran untuk penelitian selanjutnya memberikan lebih rinci tantangan dari setiap aspek kehidupan masyarakat di Indonesia. Undang-Undang Informasi dan Transaksi Elektronik menjadikan dasar keamanan bagi penggunnaan Teknologi Informasi di Indonesia.

DAFTAR PUSTAKA

[1] M. Bisri Mustofa, E. Luthfiah Dwiandrini, I. Agustin, M. Afief Esyarito, M. Anggraeni, and S. Wuryan, "MEDIA MASSA DAN CYBER CRIME DI ERA SOCIETY 5.0 (Tinjauan Multidisipliner), *AT-TANZIRJurnal Prodi Komun. dan Penyiaran Islam*, vol. 13, no. 1, pp. 77–98, 2022.

[2] Y. Samudra, A. Hidayat, and M. F. Wahyu, "AMMA : Jurnal Pengabdian Masyarakat Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital," *Januari*, vol. 1, no. 12, pp. 1594–1601, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/amma

[3] M. Irfan *et al.*, "ANCAMAN CYBERCRIME DAN PERAN CYBERSECURITY PADA E-COMMERCE : SYSTEMATIC LITERATURE REVIEW," vol. 11, 2023.

[4] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[5] H. Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya Di Indonesia," pp. 95–110, 1986.

[6] Y. Puspita, Y. Fitriani, S. Astuti, and S. Novianti, "Selamat Tinggal Revolusi Industri 4.0, Selamat Datang Revolusi Industri 5.0," *Pros. Semin. Nas. Pendidik. Progr. Pascasarj. Univ. PGRI Palembang*, pp. 1–9, 2020.

[7] B. I. Darmawan, "Simulasi dan Analisis Encryption Based Ransomware untuk Memetakan Evolusi Ransomware," 2019, [Online]. Available: https://dspace.uii.ac.id/handle/123456789/18039%0Ahttps://dspace.uii.ac.id/bitstream/handle/123456789/18039/08.naskah publikasi.pdf?sequence=12&isAllowed=y

[8] W. W. Yunanda *et al.*, "Strategi Menjaga Kedaulatan Bangsa Demi Keutuhan Negara Kesatuan Republik Indonesia Di Era Society 5.0 Dalam Perspektif Ilmu Pertahanan Dan Bela Negara," *J. Kewarganegaraan*, vol. 6, no. 1, pp. 1195–1202, 2022.

[9] R. Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia," *J. Ilm. Huk. Dirgant.*, vol. 11, no. 2, pp. 44–56, 2021.

[10] T. Yusnanto *et al.*, "'Jurnal TRANSFORMASI (Informasi & Pengembangan Iptek)' (STMIK BINA PATRIA) Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0," *J. Transform.*, vol. 17, no. 2, pp. 24–35, 2021.

[11] Satriawan, N. Husnul Khatimah, Gufran, "Sewagati : Jurnal Pengabdian Masyarakat Sosialisasi Peningnya Menjaga Privasi Dan Keamanan Digital Di Era Digital," Maret, Vol. 02, No.1, 2023, [Online]. Available : http://ejurnal.sarauinstitute.org/index.php/sewagati/article/view/10

[12] H. Sutejo, R. H. Kiswanto, R. M.H. Thamrin, "Edukasi dan Sosialisasi CyberCrimeTerhadap Keamanan Data Bagi Kalangan Guru Tingkat Sekolah Menengah Pertama di Kota Jayapura", *Pros. Semin. Nas. Corisindo. Intitut Teknologi dan Bisnis STIKOM Bali*, Agustus, 2022