Jurnal Inovasi Teknik dan Edukasi Teknologi, 2(7), 2022, 349-354
ISSN: 2797-7196 (online)
DOI: 10.17977/um068v1i72022p349-354

Peran dan Tantangan *Cyber Security* di Era *Society* 5.0

Muhammad Fahli Saputra, Aji Prasetya Wibawa*
Universitas Negeri Malang, Jl. Semarang No. 5 Malang, Jawa Timur, Indonesia
*Penulis korespondensi, Surel: aji.prasetya.ft@um.ac.id

Paper received: 06-07-2022; revised: 15-07-2022; accepted: 29-07-2022

Abstract

Merging virtual and real worlds in Society 5.0 by integrating artificial intelligence and the internet of things makes it easy for humans and becomes a solution to social problems faced in the 4.0 era. Humans will coexist with technology that is developing very rapidly, making cyber threats even more real. This study uses a qualitative descriptive approach with data sources from a literature review using a conceptual review technique to collect information about cybersecurity and society 5.0. The aim is to provide an overview of the important roles and challenges that will be faced in the development of cyber security. The result is that cyber security is a very important element to protect the entire infrastructure of society. There are several challenges in the development of cyber security, one of which is the lack of human resources who are experts in the world of cyber security and the lack of public awareness of cyber threats. Cyber security must continue to evolve following technological developments and new threats that occur so quickly.

Keywords: cyber security, society 5.0, technology

Abstrak

Penggabungan dunia maya dan *real world* pada era *Society* 5.0 dengan mengintegrasikan *artificial intelligence* dan *internet of things* memberikan kemudahan bagi manusia dan menjadi solusi dari masalah sosial yang dihadapi pada era 4.0. Manusia akan hidup bersama teknologi secara berdampingan yang berkembang sangat pesat, membuat ancaman dunia maya semakin nyata. Metode deskriptif kualitatif digunakan pada penelitian ini dengan sumber data dari tinjauan literatur dengan teknik *conceptual review* untuk mengumpulkan informasi mengenai keamanan siber dan masyarakat 5.0. Tujuannya adalah untuk memberikan gambaran mengenai peran penting serta tantangan yang akan dihadapi dalam perkembangan *cyber security.* Hasilnya adalah *cyber security* merupakan unsur yang sangat penting untuk melindungi seluruh infrastruktur masyarakat. Terdapat beberapa tantangan dalam perkembangan *cyber security,* salah satunya adalah sumber daya manusia yang ahli terhadap dunia keamanan dan siber masih sangat sedikit. Selain itu juga lemahnya kesadaran masyarakat akan ancaman dunia maya. *Cyber security* harus terus berkembang mengikuti perkembangan teknologi dan ancaman baru yang begitu cepat terjadi.

Kata kunci: keamanan siber, masyarakat 5.0, teknologi

1. Pendahuluan

Teknologi informasi berkembang begitu pesat memberikan dampak yang besar ke bagi kehidupan masyarakat dalam banyak aspek, seperti aspek pendidikan, sosial budaya, ekonomi, politik hingga aspek keamanan dan pertahanan. Contoh sederhana dari dampak perkembangan teknologi ini adalah kemudahan dalam melakukan transaksi *online* hanya dalam hitungan detik. Pertumbuhan penggunaan teknologi informasi dan komunikasi meningkat secara tajam dalam tiga dekade terakhir (Castellacci & Tveito, 2018). Pada era sebelumnya, yaitu era 4.0, media sosial juga hadir disekitar kehidupan masyarakat. Media sosial memberikan dampak yang besar dalam etika dan norma yang telah ditetapkan di dalam kehidupan masyarakat. (Cahyono, 2016). Menurut laporan yang diterbitkan oleh *We Are Social* berjudul *Digital 2023 Local Country Headlines Report*, dikutip dari Kemp (2023), total pengguna aktif sosial media di Indonesia hingga Januari 2023 mencapai 167 juta orang yaitu

sebesar 60,4% dari total populasi. Hal tersebut membuktikan betapa pentingnya teknologi yang sudah tidak dapat terpisahkan dari kehidupan masyarakat.

Konsep *Society* 5.0 hadir untuk menyelesaikan masalah yang telah terjadi pada era 4.0 yang dikhawatirkan akan memberikan dampak kemunduran pada karakter umat manusia (Budi, Wira, & Infantono, 2021). Menurut Deguchi & Hirai (2020), tujuan diciptakan konsep *Society* 5.0 adalah untuk menggabungkan dunia maya dan dunia nyata menjadi kesatuan yang utuh dengan memanfaatkan teknologi. Hal ini akan memberikan kemudahan dalam kehidupan masyarakat dengan mengintegrasikan *artificial intelligence* dalam dunia nyata serta *internet of things* (IoT). Dengan kombinasi teknologi tersebut, akan menghasilkan *insight* yang berguna bagi manusia untuk mengambil suatu keputusan. Era *Society* 5.0 menerapkan konsep *human centered* yang berbasis pada teknologi, sehingga nilai sosial budaya pada masyarakat tetap terjaga dengan baik (Fukuyama, 2018).

Society 5.0 menggambarkan bahwa manusia dan teknologi akan hidup berdampingan agar kualitas hidup manusia akan terus meningkat secara berkelanjutan. Namun, ini juga akan menyebabkan munculnya tantangan terkait ancaman dunia maya karena seluruh data atau informasi akan disimpan melalui teknologi yang rentan terhadap pencurian data. Teknologi ini juga dapat digunakan oleh pihak tidak bertanggungjawab untuk menyebarkan berbagai macam hal-hal negatif, misalkan saja seperti berita palsu (hoax), propaganda, hujatan serta hal lainnya dengan tujuan mengganggu stabilitas keamanan dan politik suatu negara (Siagian, Budiarto, & Simatupang, 2018).

Peneliti dari perusahaan *cyber security* terkemuka, Kaspersky (2022), memprediksi bahwa pada tahun 2023 serangan *malware* akan meningkat pada sistem kontrol industri. Serangan ini meningkat karena terjadi digitalisasi serta meningkatkan efisensi yang lebih tinggi dalam teknologi IoT. Pada *press release* tersebut, Kaspersky juga menyebutkan bahwa Indonesia menempati posisi kedua negara yang paling sering diserang terhadap *Computerized Maintenance Management Systems (CMMS)* pada awal tahun 2022 . Tentunya ini akan menjadi ancaman lebih besar jika suatu saat teknologi akan dikombinasikan langsung dalam kehidupan masyarakat era *Society* 5.0.

Dikutip dari Budi, Wira, & Infantono (2021), Hasyim Gautama menyebutkan beberapa permasalahan tentang *cyber security* di Indonesia, salah satunya adalah karena pemahaman penyelenggara negara masih dinilai lemah terhadap *security* yaitu tentang pembatasan layanan jika server berada di luar negara Indonesia serta juga dibutuhkan penerapan *secured* system*.* Kemudian masalah selanjutnya adalah pola *cyber crime* sangat cepat terjadi sehingga sulit untuk ditangani. Masalah lainnya adalah tata kelola lembaga *cyber security* nasional yang masih kurang, rendahnya kesadaran terhadap *cyber threat* global yang mampu melemahkan bahkan melumpuhkan beberapa infrastruktur penting suatu negara serta masih sedikit industri yang mampu dalam mengembangkan *hardware* yang berkaitan dengan teknologi informasi.

Saat ini, Indonesia sangat membutuhkan dasar hukum mengenai *cyber security* dalam menangani serangan siber yang terjadi dalam wilayah hukum Indonesia. Perlunya pembelajaran mengenai dunia *cyber* di sekolah untuk meningkatkan *awareness* orang-orang terhadap pentingnya keamanan saat memasuki dunia maya. *Cyber security* menjadi tantangan yang besar bagi masyarakat *Society* 5.0 karena akan sangat rentan terhadap ancaman yang

masuk dari teknologi, maka dari itu harus dilakukan upaya keamanan nasional Indonesia terhadap peningkatan *cyber attack* secepat mungkin.

Berdasarkan hasil penjabaran di atas, maka tujuan penelitian ini dalam mendeskripsikan peran dan tantangan terhadap *cyber security* atau keamanan siber di era *Society* 5.0 menjadi sangat penting agar dapat dijadikan salah satu acuan dalam meningkatkan pengetahuan akan *cyber security*, terutama bagi masyarakat.

2. Metode

Penelitian ini menerapkan *approach method* yaitu deskriptif kualitatif. Dalam tulisannya, Moleong (2000) menjelaskan bahwa penelitian kualitatif bertujuan untuk memahami secara holistik (menyeluruh) hal yang dialami oleh subjek dari penelitian dengan mendeskripsikan data menggunakan kata-kata serta menggunakan berbagai metode alamiah. Dalam sebuah penelitian, data merupakan unsur yang sangat penting karena kualitas penelitian sangat bergantung pada data. Sumber data pada penelitian ini diambil melalui studi literatur dengan teknik *conceptual review*, yaitu metode untuk mengumpulkan data yang sesuai dengan konteks penelitian yang bersumber dari bahan pustaka literatur, buku, penelitian-penelitian terdahulu dan lain-lain. *Conceptual review* dapat memberikan pemahaman tentang suatu isu melalui proses cakupan konseptual (Petticrew & Roberts, 2008). Penelitian ini mengumpulkan berbagai macam literatur akademis yang relevan dengan *cyber security* dan *Society* 5.0 untuk memperoleh pengetahuan baru mengenai *cyber security* yang dikombinasikan dengan pandangan *Society* 5.0. Prosedur yang diterapkan untuk memilih literatur dalam penelitian ini dijelaskan pada tabel 1 di bawah.

Tabel 1. Langkah tinjauan literatur

Tahap	Penjelasan
Menentukan keyword pencarian yang berkaitan dengan penelitian	Keyword yang digunakan untuk mencari literatur yang relevan adalah Society 5.0, cyber security, keamanan siber, internet serta privasi data.
Menelusuri literatur dari berbagai sumber	Literatur akademis dicari menggunakan bantuan Google Scholar, Mendeley, serta Publish or Perish 7. Literatur yang dipilih dalam penelitian ini adalah literatur terbuka yang dapat diakses oleh siapa saja. Proses penelusuran dilakukan pada rentang tanggal 20 Februari 2023 – 2 Maret 2023.
Menyaring literatur yang telah didapatkan berdasarkan kriteria inklusi	Berikut kriteria literatur yang dijadikan sebagai acuan terhadap pengembangan penelitian ini: Literatur membahas tentang Society 5.0 Literatur berfokus mengenai masalah privasi dan keamanan data. Literatur membahas tentang cyber security atau keamanan siber.
Menganalisis literatur akademis yang didapatkan	Jika literatur telah memenuhi kriteria inklusi, dilakukan analisis kemudian diambil intisari dari literatur tersebut yang akhirnya dapat dikaji terkait berbagai aspek yang tentunya mendukung penelitian ini.
Memastikan kualitas literatur akademis	Kualitas analisis literatur akan diperiksa lagi secara berulang kali agar relevan dengan topik penelitian ini.
Menulis artikel tinjauan literatur	Tujuan dari penulisan laporan tinjauan literatur adalah untuk mendeskripsikan hasil analisis secara keseluruhan yang ditulis dalam artikel ini pada bagian 3.

Sumber: Francis & Baldesari (2006), dimodifikasi oleh penulis.

Berbagai gagasan utama pada literatur yang didapatkan dari prosedur tersebut akan dikaji sehingga menghasilkan sebuah pandangan tentang *cyber security* dalam pandangan *Society* 5.0.

3. Hasil dan Pembahasan

3.1. *Cyber Crime* dan *Cyber Security* di Era *Society* 5.0

Tidak dapat dipungkiri bahwa risiko keamanan akan terjadi lebih tinggi pada *Society* 5.0 akibat dari konektivitas yang lebih baik. Teknologi keamanan akan lebih sulit diterapkan karena melibatkan kombinasi data dengan ruang empat dimensi. Situasi ini dapat memberikan banyak jalan bagi peretas untuk menyerang sebuah sistem. Oleh karena itu, aspek keamanan dan privasi harus diperhatikan (Liu dkk., 2019). Manajemen *cyber security* akan menjadi sebuah tantangan di *Society* 5.0, terutama dengan meningkatnya *cyber-attack* terhadap dunia industri (Paez & Tobitsch, 2017). Menurut Trautman & Ormerod (2017), konsep *cyber security* yang terus berkembang akan menghadapi tantangan baru oleh perkembangan teknologi yang begitu pesat. Pada *Society* 5.0 diperkirakan akan kesenjangan antara hukum tentang *security* dengan kemajuan teknologi akan lebih dalam (Althabhawi, Zainol, & Bagheri, 2022).

Cyber-attack pada *Society* 5.0 tentunya jauh lebih berbahaya daripada era revolusi industri 4.0. Alasannya karena sejumlah besar data akan dapat dikontrol oleh peretas. Menyerang penyimpanan data yang besar akan memengaruhi lebih banyak orang dengan lebih banyak informasi yang dicuri. Selain itu, semua orang akan saling terhubung melalui internet, sehingga peretas dengan sangat mudah untuk masuk ke dalam jaringan tersebut.

Dikutip dari Mustofa, dkk. (2022), Badan Siber dan Sandi Negara (BSSN) melaporkan terjadinya *cyber-attack* sebanyak 12,8 juta kali pada tahun 2018. Kemudian serangan meningkat sangat drastis pada tahun 2019 menjadi 98,2 juta kali. Pada tahun 2020, serangan menurun menjadi sebesar 74,2 juta kali. Dari data ini, dapat disimpulkan bahwa Indonesia termasuk negara dengan tingkat serangan yang cukup tinggi.

Terdapat banyak sekali jenis kejahatan siber yang tengah terjadi di sekitaran kehidupan masyarakat, yang salah satunya adalah sebagai berikut.

1. *Scam* berbasis komputer, misalnya seperti pencurian informasi, pencurian kartu kredit, penipuan menggunakan media sosial, dan lain sebagainya.
2. *Cyber terrorism* yang mengarah ke tindak terorisme menggunakan komputer.
3. *Cyber warfare* yaitu peperangan melalui dunia maya.
4. *Cyber-attacks* yaitu penyerangan ke sebuah sistem komputer.

Berdasarkan penjabaran para ahli di atas, maka *cyber security* adalah unsur yang sangat penting dan harus segera dilaksanakan di era *Society* 5.0 untuk menjaga keamanan digital masyarakat karena seluruh aktivitas akan terhubung melalui internet, seperti contohnya melakukan transaksi, berkomunikasi dan lain sebagainya.

3.2. Peran Penting *Cyber Security* di Era *Society* 5.0

Menurut Siagan, dkk. (2018) *cyber security* berperan penting dalam mendeteksi, menangkal dan meminimalisir risiko terjadinya gangguan dari *cyber-attack* maupun *cyber*

threat yang akan mengancam keamanan seluruh komponen *cyber* itu sendiri, meliputi perangkat lunak dan keras, data atau informasi serta infrastruktur. Komponen utama dari sebuah *cyber security* adalah kerahasiaan (*confidentiality),* integritas (*integrity),* serta ketersediaan (availability).

Jika dikaitkan dengan *Society* 5.0, maka peran *cyber security* tentunya untuk menjaga seluruh infrastruktur agar berjalan dengan baik tanpa gangguan apapun. Serangan siber tentunya dapat mengganggu stabilitas sebuah negara, dengan adanya pengelolaan *cyber security* yang baik, maka akan meminimalisir terjadinya kejahatan antara dunia maya dan nyata.

3.3. Tantangan *Cyber Security* atau Keamanan Siber di Era *Society* 5.0

Ada banyak sekali tantangan yang akan dihadapi pada era *Society* 5.0. Jika dilihat dari perspektif pemerintah, tantangan yang dihadapi yaitu sumber daya manusia yang ahli di dunia teknologi dan keamanan yang mampu merancang dan mengimplementasikan sistem *cyber security* di Indonesia sangatlah sedikit. Dengan perkembangan teknologi yang begitu cepat, maka diperlukan juga pembaruan secara berkala terhadap teknologi *cyber security.* Jika para ahli keamanan tidak mengikuti trend perkembangan teknologi, maka tentunya teknologi *cyber security* yang telah ada, tidak akan mampu untuk menghadapi ancaman-ancaman baru yang semakin berkembang.

Menurut Hasyim Gautama, dikutip dari Ardiyanti (2014) ada beberapa *obstacle* atau tantangan yang akan dihadapi terhadap perkembangan *cyber security* dalam skala nasional, diantaranya:

1. Penyelenggara negara masih memiliki pemahaman yang lemah tentang masalah *cyber security.*
2. Beberapa layanan internet masih menggunakan server di luar negeri.
3. Kurangnya sistem yang aman.
4. Sering terjadinya kejahatan dunia maya yang membuatnya sulit untuk ditangani.
5. Masalah dengan tata kelola lembaga keamanan siber nasional.
6. Lemahnya kesadaran akan ancaman serangan dunia maya.
7. Kurangnya industri yang mengembangkan perangkat keras untuk memperkuat keamanan dunia maya.

4. Simpulan

Dari penjabaran penelitian di atas, disimpulkan bahwa era Society 5.0 akan memberikan kemudahan bagi manusia serta menjadi solusi dari masalah social yang terjadi di era 4.0. Dengan konsep penggabungan dunia maya dan nyata, tentunya manusia akan terkoneksi satu sama lain melalui internet. Maka dari itu, cyber security merupakan unsur yang sangat penting untuk melindungi seluruh infrastruktur masyarakat. Namun, terdapat banyak tantangan dalam meningkatkan cyber security khususnya di Indonesia. Cyber security harus terus berkembang mengikuti perkembangan teknologi dan ancaman baru yang begitu cepat terjadi. Diperlukan sumber daya manusia yang mampu untuk merancang sistem keamanan menggunakan sebuah teknologi.

Daftar Rujukan

Althabhawi, N. M., Zainol, Z. A., & Bagheri, P. (2022). Society 5.0: A New Challenge to Legal Norms. *Sriwijaya Law Review*, *6*(1), 41–54. https://doi.org/10.28946/SLREV.VOL6.ISS1.1415.PP41-54

Ardiyanti, H. (2014). Cybersecurity dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica*, *5*(1), 1–26.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Cahyono, A. S. (2016). Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia. *Publiciana*, *9*(1), 140–157.

Castellacci, F., & Tveito, V. (2018). Internet use and well-being: A survey and a theoretical framework. *Research Policy*, *47*(1), 308–325. https://doi.org/10.1016/j.respol.2017.11.007

Deguchi, A., & Hirai, C. (2020). Correction to: Society 5.0. Dalam *Society 5.0* (hlm. C1–C1). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-2989-4_9

Francis, S., & Baldesari. (2006). *Systematic Reviews of Qualitative Literature*. Oxford: UK Cochrane Centre.

Fukuyama, M. (2018). Society 5.0: Aiming for a New Human-Centered Society. *Japan SPOTLIGHT*, 47–50.

Kaspersky. (2022). Kaspersky predicts shifts in threat landscape to industrial control systems in 2023. Diambil 2 Maret 2023, dari https://www.kaspersky.com/about/press-releases/2022_kaspersky-predicts-shifts-in-threat-landscape-to-industrial-control-systems-in-2023

Kemp, S. (2023). DIGITAL 2023: Local Country Headlines Report. Diambil 2 Maret 2023, dari Datareportal website: https://datareportal.com/reports/digital-2023-local-country-headlines

Liu, H., Ning, H., Mu, Q., Zheng, Y., Zeng, J., Yang, L. T., … Ma, J. (2019). A review of the smart world. *Future Generation Computer Systems*, *96*, 678–691. https://doi.org/10.1016/J.FUTURE.2017.09.010

Moleong, L. J. (2000). *Metode Penelitian Kulitatif*. Bandung: PT Remaja Rosdakarya.

Mustofa, M. B., Dwiandrini, E. L., Agustin, I., Esyarito, M. A., Anggraeni, M., & Wuryan, S. (2022). Media Massa dan Cyber Crime di Era Society 5.0 (Tinjauan Multidisipliner). *Jurnal Prodi Komunikasi dan Penyiaran Islam*, *13*(1), 77–98.

Paez, M., & Tobitsch, K. (2017). The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues. *New York Law School Law Review*, *62*.

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences: A Practical Guide. *Systematic Reviews in the Social Sciences: A Practical Guide*, 1–336. https://doi.org/10.1002/9780470754887

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Peperangan Asimetris*, *4*(3).

Trautman, L. J., & Ormerod, P. (2017). Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2982629