PENGGUNAAN AGEN BERBASIS INTELIJEN UNTUK MENANGANI KEJAHATAN SIBER

Oleh
Muhamad Arif Budiman
Sekolah Kajian Stratejik dan Global, Universitas Indonesia
Email: muhaarifb30@gmail.com

Abstrak

Perkembangan pesat teknologi informasi dan komunikasi telah mendorong semakin berkembangnya kejahatan siber. Sebagai jenis kejahatan yang berbeda dari kejahatan konvensional, maka penanganan kejahatan siber memerlukan cara khusus. Tulisan ini bertujuan untuk meneliti agen berbasis intelijen untuk penanganan kejahatan siber, Indonesia dengan fokus kepada penggunaan *chatbot*. Metode yang digunakan adalah metode kepustakaan (*library research*). Data yang bersumber dari berbagai buku, jurnal dan sumber internet kemudian dianalisa dengan metode deskriptif analisis. Hasil penelitian menunjukkan bahwa perkembangan AI yang ada saat ini telah memungkinkan penggunaannya untuk melakukan *crime data mining*. Hal ini salah satunya dilakukan dengan menggunakan *chatbot* yang merupakan salah satu jenis agen berbasis intelijen. Pemanfaatan chatbot dalam kepolisian memiliki kemungkinan untuk dikembangkan sebagai deteksi kejahatan siber dan cara pengumpulan alat bukti. Hal ini dilakukan dengan mengembangkan kerangka kerja *chatbot* metodologi dan prosedur pengumpulan bukti di dark web dan praktik digital forensik.

Kata kunci: Agen Berbasis Intelijen, Chatbot, *Crime Data Mining,* Kejahatan Siber

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang ada sekarang ini telah memunculkan berbagai tantangan baru akibat dampak buruk yang dihasilkan dari penyalahgunaannya. Hal ini kemudian menyebabkan berbagai pihak yang tidak bertanggungjawab mengambil keuntungan dengan cara-cara yang merugikan banyak orang. Kejahatan siber (*cyber crime*) merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi, komputer, dan telekomunikasi, baik untuk memperoleh keuntungan ataupun tidak dengan merugikan pihak lain (Marufah, Rahmat, & Widana, 2020). Kejahatan ini melibatkan berbagai bentuk kejahatahn yang yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer (Chintia, Nadiah, Ramadhani, Haedar, & Febriansyah, 2019).

Jumlah kejahatan siber yang terjadi di Indonesia tidak dapat dibilang sedikit. Berdasarkan pada data yang dimiliki oleh Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa terdapat 888 juta serangan siber yang terjadi di Indonesia dari Januari hingga Agustus 2021 (Mashabi, 2021). Hal tersebut kemudian menunjukkan tingkat keparahan kejahatan siber yang terjadi di Indonesia. Pemerintah Indonesia pun tidak tinggal diam dan melakukan berbagai upaya untuk dapat menangani kejahatan siber yang ada di Indonesia. Hal ini dilakukan dengan menerbitkan Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diperbaharui oleh Undang-undang No. 19 Tahun 2016. Perundangan tersebut kemudian digunakan sebagai dasar penanganan kejahatan siber yang ada di Indonesia.

Selain produk hukum tersebut, penegakan hukum telah dilakukan oleh Polri sebagai kepolisian Indonesia untuk melakukan

penanganan kejahatan siber. Hal ini salah satunya dengan membentuk Direktorat Tindak Pidana Siber (Dittipidsiber) yang merupakan satuan kerja di bawah Bareskrim Polri dan memiliki tugas untuk melakukan penegakan hukum terhadap kejahatan siber. Selain itu, Polri juga melakukan upaya untuk mengoptimalkan kualitas proses penyidikan kejahatan siber dengan pelaksanaan pelatihan terhadap anggotanya (Nahwan, Nurhayani, Nugroho, & Srimurni, 2021). Namun kemudian upaya tersebut tampaknya masih perlu ditingkatkan dan didorong dengan strategi lainnya.

Berdasarkan pada penelitian yang dilakukan oleh Noviantini, Remaja, dan Mariadi (2021), belum optimalnya kepolisian dalam melakukan penanganan terhadap kejahatan siber datang dari faktor penegak hukumnya. Hal ini utamanya berkaitan dengan pendidikan khusus yang belum dimiliki oleh satuan fungsi khusus siber. Selain itu, terdapat kebutuhan akan sarana dan prasarana yang lebih memadai terutama di daerah untuk dapat meningkatkan kelancaran proses penyelidikan kejahatan dunia maya. Sarana dan prasarana yang paling dibutuhkan adalah laboratorium digital forensik yang dianggap memiliki peran yang besar dalam penyedikan berbagai tindak pidana siber.

Kejahatan siber merupakan jenis kejahatan yang memerlukan perhatian khusus karena jenisnya yang memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional (Chintia, Nadiah, Ramadhani, Haedar, & Febriansyah, 2019). Kejahatan dunia maya harus menjadi fokus utama lembaga penegak hukum. Dalam hal ini, berbagai lembaga pemerintahan yang berada di sektor keamanan, bersama dengan badan intelijen perlu berkolaborasi dengan ahli yang terampil secara teknis agar dapat mengadopsi dan membingkai berbagai teknologi baru yang muncul untuk mengatasi berbagai jenis kejahatan siber. Keamanan siber kemudian dapat dicapai dengan perencanaan dan penerapan strategi yang tepat untuk mengatasi masalah kejahatan siber (Almansoori, Alshamsi, Abdallah, & Salloum, 2021).

Perkembangan kecerdasan buatan (*artificial intelligence/AI*) sekarang ini telah menyebabkan berbagai kemudahan dengan menyediakan sistem operasi intelektual dan asisten digital. Pemanfaatan AI bahkan telah memungkinkan bagi robot untuk melakukan fungsi dasar polisi. Saat ini polisi sudah menggunakan robot untuk melakukan operasi pencarian dan penyelamatan, untuk membuang bahan peledak dalam kegiatan teroris dan bahkan untuk menghancurkan penjahat bersenjata (Radulov, 2019). Lebih dari itu, karena perkembangan luas dari AI itu sendiri, maka AI telah berkembang sehingga dapat digunakan dalam berbagai bentuk. Paradigma AI telah mengubah praktik kepolisian, pengawasan, dan peradilan pidana melalui modalitas pemantauan yang tersebar berdasarkan prediksi dan pencegahan. Selain itu, hal ini kemudian dapat digunakan untuk melakukan penanganan terhadap kejahatan siber. Penelitian yang dilakukan oleh Sivčević, et.al (2020) menunjukkan bahwa terdapat kemungkinan penggunaan agen berbasis intelijen untuk melakukan layanan publik elektronik dengan menggunakan kecerdasan buatan yang sesuai seperti *chatbot*. Berdasarkan penelitian tersebut maka terdapat pula kemungkinan kepolisian menggunakan agen berbasis intelijen untuk melakukan penanganan kejahatan siber.

Tulisan ini bertujuan untuk menganalisa penggunaan agen berbasis intelijen untuk penanganan kejahatan siber di Indonesia dengan fokus kepada penggunaan *chatbot*. Tulisan ini berkontribusi kepada literatur dengan cara menyediakan wawasan mengenai kemungkinan penggunaan agen berbasis intelijen chatbot dalam deteksi kejahatan siber melalui data mining. Tulisan ini akan disusun berdasarkan urutan pada bagian selanjutnya menjelaskan metode yang digunakan. Setelah itu akan dijelaskan temuan dan diskusi, dan bagian terakhir menjelaskan kesimpulan penelitian.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

LANDASAN TEORI

Teori Intelijen

Michael Warner (2006) Office of the Director of National Intelligence, dalam presentasinya mengenai Intelijen mengatakan bahwa Intelijen memiliki banyak makna bagi beberapa orang. Mengartikan Intelijen kedalam 1 (satu) definisi akan sangat sulit dilakukan, terdapat 2 (dua) definisi yang sering digunakan secara umum yaitu "Intelijen bagi Pengambil Keputusan" dan definisi lainnya "Intelijen adalah aktifitas rahasia suatu Negara untuk memahami dan mempengaruhi entitas asing". Mengutip pemikiran Sun Tzu (1963), yang menambahkan istilah "Spionase" dalam Intelijen, yang merupakan penerjemahan atas informasi dan aksi, lebih lanjut terdapat doktrin yang dikatakan oleh Sun Tzu, Intelijen harus bekerja secara rahasia "Ketika agen tipe ini bekerja secara simultan dan tidak ada yang mengetahui metode operasi, mereka disebut "The Devine Skein" dan merupakan harta karun atas kedaulatan. Hank Prunckun (2010), salah satu penulis tentang Intelijen dalam bukunya membuat 4 (empat) definisi dari Intelijen:

1. Tindakan
2. Tempat produksi pengetahuan
3. Organisasi yang menangani pengetahuan
4. Laporan yang dihasilkan dari proses ataupun organisasi

METODE PENELITIAN

Metode penelitian yang digunakan untuk menyusun tulisan ini adalah metode kepustakaan (*library research*). Hal ini dilaksanakan dengan mengumpulkan berbagai referensi bacaan yang relevan dengan permasalahan yang diteliti, kemudian dilakukan pemahaman cara teliti dan hati-hati sehingga mendapatkan sebuah temuan-temuan penelitian (Zed, 2003). Data dikumpulkan dari berbagai literatur seperti buku, jurnal baik nasional maupun internasional, serta sumber internet. Hal ini kemudian dilanjutkan dengan analisa yang dilakukan dengan menggunakan metode deskriptif analisis. Berdasarkan metode analisa tersebut maka data hasil pengamatan dituangkan kedalam bentuk tesis untuk memaparkan permasalahan yang diteliti.

HASIL DAN PEMBAHASAN

1. Kecerdasan buatan dan penanggulangan kejahatan

Kecerdasan buatan mengacu pada simulasi kecerdasan mansia pada mesin yang di program untuk berikir manusia dan meniru tindakannya, karakteristik AI sendiri adalah kemampuannya untuk merasionalisasi dan mengambil tindakan yang memiliki peluang terbaik untuk mencapai tujuan tertentu (Rachmadie, 2020). Hal ini kemudian dimanfaatkan dalam sektor keamanan untuk mengumpulkan, menyortir, dan mengelola data yang ada di ruang informasi. Hal ini kemudian diharapkan untuk dapat mengoptimalkan kinerja kepolisian dengan cara yang berkualitas, tepat waktu, dan efektif dalam menjamin keamanan nasional dan sipil (Radulov, 2019).

Menurut Radulov (2019) terdapat beberapa cara yang dapat digunakan untuk memanfaatkan AI dalam penanggulangan kejahatan. Hal ini diantaranya dilakukan dengan pengumpulan data, pendeteksian tindak pidana, pencegahan kejahatan siber dan lain sebagainya. AI dipandang dapat membantu organisasi untuk mencegah kejahatan siber dengan cara melatihnya untuk mengenali kata kunci atau topik yang terkait dengan konten berbahaya yang kemudian digunakan untuk menghentikan potensi serangan dunia maya. Selain itu, Machine Learning, algoritme komputer yang memungkinkan AI melakukan pembelajaran telah memungkinkan AI untuk bekerja dengan sejumlah besar data. Hal tersebut kemudian dapat dimanfaatkan untuk menyelidiki dan mencegah kejahatan (Radulov, 2019).

Penyelidikan kejahatan dan pengumpulan informasi yang berkaitan dengan tindak pidana yang dilakukan oleh kepolisian dapat dilakukan dengan bantuan AI. Pengumpulan informasi mengenai situasi kejahatan termasuk menemukan hubungan tersembunyi antara organisasi dan individu

yang melakukan kejahatan dapat dilakukan dengan kecerdasan buatan (Radulov, 2019). Hal ini salah satunya berkat adanya fungsi *data mining* yang disediakan AI. *Data mining* didefinisikan sebagai identifikasi struktur yang menarik dalam data, di mana struktur menunjukkan pola, model statistik atau prediksi data, dan hubungan antara bagian-bagian data (Fayyad & Uthurusamy, 2002).

Data mining kemudian dapat digunakan untuk deteksi, pencegahan, dan pemberantasan kejahatan. Penelitian yang dilakukan oleh Chen, et al. (2003) menyebutkan bahwa *crime data mining* dapat digunakan untuk ekstraksi entitas untuk laporan narasi polisi, mendeteksi penipuan identitas kriminal dengan pendekatan algoritma, analisis *authorship* dalam kejahatan dunia maya, dan analisis jaringan kriminal. Berkaitan dengan kejahatan siber, aktivitas di dunia maya kebanyakan memiliki sifat anonim yang kemudian membuat penanganan kejahatan siber menjadi semakin rumit dan harus bergantung pada upaya manual. Namun hal ini sangat dibatasi oleh banyaknya pesan dan ID pelaku yang terus berubah. Oleh karena itu, diusulkan untuk kerangka analisis authorship yang dapat digunakan untuk secara otomatis melacak identitas penjahat cyber melalui pesan yang mereka posting di Internet. Berdasarkan pada kerangka tersebut, tiga jenis fitur pesan, termasuk penanda gaya, fitur struktural, dan fitur khusus konten, diekstraksi dan algoritma pembelajaran induktif digunakan untuk membangun model berbasis fitur untuk mengidentifikasi authoship pesan ilegal (Chen, et al., 2003).

2. Agen berbasis intelijen

Secara umum, istilah "agen" dapat dilihat sebagai suatu entitas yang melakukan kegiatan tertentu sebagai perwakilan atas nama seseorang. Agen pada umumnya mengacu pada entitas yang beroperasi secara mandiri di suatu lingkungan, beradaptasi dengan lingkungan tersebut, memiliki kemampuan untuk memahami lingkungan, mengubah keadaan lingkungan tersebut, dan memiliki kemampuan untuk belajar (Kuk, Stanojević, Jovanović, & Nedeljković, 2018). Agen dapat dibedakan menurut beberapa kriteria Operasi agen dapat ditinjau dalam lingkungan yang diberikan. Keadaan lingkungan berubah seiring dengan interaksinya dengan lingkungan tersebut. Karakteristik agen berbasis intelijen menurut Sivčević, et.al (2020) dapat diperhatikan pada Tabel 1.

Tabel 1. Karakteristik agen berbasis intelijen

Karakteristik	Definisi	Tipe
Mobile	Agen dapat berpindah dari satu node jaringan ke nodus lainnya. data, yaitu atribut internal yang mewakili pengetahuan yang dimiliki agen	Mobile agent
Rationality	Agen harus selalu melakukan tindakan yang akan memaksimalkan hasil yang diharapkan, dengan demikian menggunakan pengetahuannya sendiri tentang keadaan lingkungan saat ini dan masa depan	Rationality agent
Benevolence	Target agen tidak boleh saling bertentangan jika agen diharapkan memaksimalkan hasil yang diharapkan.	Hybrid agent

Sumber (Sivčević, Košanin, Nedeljković, Nikolić, Kuk, & Nogo, 2020)

Pemanfaatan agen berbasis kecerdasan buatan diantaranya adalah sebagai berikut (Piscopo, Siebes, & Hardman, 2017):

a. Chatbots: AI dapat digunakan untuk memahami pola komunikasi sehari-hari menggunakan chatbots
b. Sinyal Lalu Lintas Adaptif: Lalu lintas kota pasti dapat mempengaruhi kehidupan kita, arus lalu lintas dan sensor dapat meningkatkan fungsi transportasi umum
c. Pengawasan dan Keamanan: Kehadiran kamera telah membuat peningkatan keselamatan publik, mengurangi tingkat kejahatan layanan polisi Cerdas, dan menangkap teroris. Pembelajaran mesin dan AI akan membantu meningkatkan pengenalan wajah, pelacakan, dan aspek deteksi keamanan lainnya
d. Air dan Listrik: AI sedang diterapkan pada pengukuran air untuk mengekang kelebihan air dan menemukan kebocoran. Kota-kota menggunakan jaringan

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

pintar/jaringan listrik untuk mengelola daya dengan lebih baik

e. Keamanan Publik: dapat sepenuhnya direvolusi jika lembaga penegak hukum menerapkan pemodelan prediktif dan kerangka kerja AI untuk menjalankan pemeriksaan terhadap basis data kriminal. Teknologi pembaca plat nomor (LPR) dapat digunakan oleh polisi untuk menemukan mobil curian dan mengidentifikasi registrasi yang kadaluwarsa.

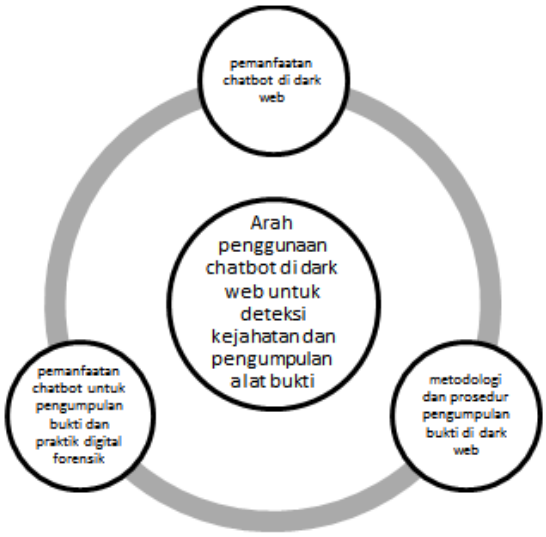
3. Pemanfaatan agen berbasis intelijen *chatbot* dalam deteksi kejahatan siber

Agen percakapan otomatis atau chatbot adalah sistem komputer yang meniru percakapan alami dengan pengguna manusia melalui gambar dan bahasa tertulis atau lisan (Laranjo, et al., 2018). Kemunculan chatbot ini menunjukkan kemajuan terbaru dalam AI yang memungkinkan interaksi yang semakin alami antara manusia dan rekan agen mesinnya. Komunikasi antara manusia-mesin ini menjadi lebih kompleks dan canggih, terutama melalui kemajuan pembelajaran mesin dengan penerapan jaringan saraf. Hal ini tercermin dari meningkatnya jumlah agen percakapan yang bertujuan untuk pertukaran seperti manusia di bidang-bidang seperti e-commerce, perjalanan, pariwisata, dan perawatan kesehatan. Contoh terkenal dari chatbot cerdas tersebut adalah Microsoft Cortana, Amazon Alexa, atau Apple Siri (Schachner, Keller, & Von Wangenheim, 2020).

Berdasarkan penelitian yang dilakukan oleh Sivčević, et.al (2020) penerapan chatbot dalam kepolisian dapat memberikan efek pada peningkatan tingkat kepercayaan warga terhadap kepolisian. Implementasi chatbots dalam pekerjaan polisi akan mengubah komunikasi antara warga dan otoritas polisi secara total. Hal ini disebabkan karena chatbot telah merevolusi interaksi manusia, yaitu antara warga sipil dan polisi. Oleh karena itu, dengan chatbot maka warga sipil dan polisi dapat berkomunikasi dalam bahasa alami. Chatbot dapat menjadi layanan yang didukung oleh aturan dan terkadang kecerdasan buatan yang berinteraksi dengan masyarakat melalui antarmuka obrolan. Chatbots dapat meningkatkan hubungan polisi-masyarakat dan mendapatkan efisiensi dalam proses menerima panggilan dengan penelepon.

Namun kemudian pemanfaatan chatbot dalam kepolisian memiliki kemungkinan untuk dikembangkan sebagai deteksi kejahatan siber. Hal ini didasarkan pada gagasan bahwa chatbot otomatis dapat bertindak secara independen dan belajar dari pengalaman mereka sendiri dan dapat menciptakan strategi pencegahan kejahatan baru. Chatbot digunakan sebagai agen rahasia untuk mendeteksi kejahatan. Dengan cara tersebut, chatbot yang biasanya digunakan untuk tujuan layanan pelanggan, perutean permintaan, pengumpulan informasi kemudian dapat diperluas fungsinya menjadi penyelidikan kejahatan dan identifikasi potensi pelaku kejahatan (Stănilă, 2020).

Berdasarkan hal tersebut Gendi dan Muntenau (2021) mengusulkan untuk menerapkan interaksi antara tiga domain untuk menggambarkan kelayakan penggunaan chatbot untuk deteksi kejahatan dan pengumpulan alat bukti. Interaksi tersebut dapat dilihat pada Gambar 1. Dalam hal ini diusulkan untuk menerapkan chatbot dengan tiga cara utama yaitu pemanfaatan chatbot di dark web, metodologi dan prosedur pengumpulan bukti di dark web, dan pemanfaatan chatbot untuk pengumpulan bukti dan praktik digital forensik. Implementasi chatbot di dark web dapat memungkinkan akses cepat terhadap data, evaluasi informasi, dan eksekusi tugas. Dengan menerapkan chatbot di dark web, seseorang dapat segera mendeteksi URL yang mudah menguap dan dengan cepat hilang (Gendi & Munteanu, 2021). Hal ini berarti penelusuran kejahatan siber dapat dilakukan dengan cara yang lebih mudah dengan memanfaatkan chatbot.



Gambar 1. Interaksi tiga domain untuk menggambarkan kelayakan penggunaan chatbot di dark web untuk deteksi kejahatan dan pengumpulan alat bukti (Gendi & Munteanu, 2021)

Selain itu, dengan menerapkan chatbot di dark web, seseorang dapat memfasilitasi berbagi informasi yang efisien sambil meminimalkan keterampilan teknis yang diperlukan untuk pengumpulan data dan informasi. Terakhir, sebagai implementasi praktis dari AI, chatbots dapat digunakan untuk mendeteksi aktivitas kriminal. Secara khusus, Gendi dan Muntenau (2021) berpendapat bahwa chatbots dapat diimplementasikan dengan tujuan mengumpulkan catatan aktivitas ilegal dan mengidentifikasi pelaku dalam operasi mereka. Eksploitasi fungsi chatbot juga dapat dilakukan dengan analisis data cerdas di berbagai bidang kegiatan kepolisian. Analisis polisi terhadap data yang dikumpulkan oleh agen berbasis kecerdasan buatan dapat dieksploitasi untuk melakukan pengumpulan dan analisis data dari kegiatan kriminal (Sivčević, Košanin, Nedeljković, Nikolić, Kuk, & Nogo, 2020).

4. Kesimpulan

Kejahatan siber merupakan jenis kejahatan yang berbeda dari kejahatan konvensional. Oleh karena itu, memerlukan upaya penanganan yang berbeda-beda. Tulisan ini telah melakukan tinjauan penggunaan agen berbasis intelijen untuk dalam penanganan kejahatan siber, terutama dengan menggunakan chatbot. Tinjauan menunjukkan hasil bahwa perkembangan AI yang ada saat ini telah memungkinkan penggunaannya untuk melakukan *crime data mining*. Agen berbasis intelijen dapat dimanfaatkan untuk hal tersebut, terutama chatbot yang dapat berfungsi untuk memahami pola komunikasi sehari-hari. Chatbot dalam kepolisian memiliki kemungkinan untuk dikembangkan sebagai deteksi kejahatan siber. Hal ini dapat dilakukan dengan mengembangkan kerangka kerjanya untuk dapat memanfaatkan chatbot di dark web, diterapkan sebagai metodologi dan prosedur pengumpulan bukti di dark web, dan pemanfaatan chatbot untuk pengumpulan bukti dan praktik digital forensik. Dengan cara tersebut, chatbot kemudian dapat difungsikan sebagai deteksi kejahatan siber dan cara pengumpulan alat bukti.

DAFTAR PUSTAKA

[1] Almansoori, A., Alshamsi, M., Abdallah, S., & Salloum, S. A. (2021). Analysis of Cybercrime on Social Media Platforms and Its Challenges. *The International Conference on Artificial Intelligence and Computer Vision* (pp. 615-625). Springer, Cham.

[2] Chen, H., Chung, W., Qin, Y., Chau, M., Xu, J. J., Wang, G., et al. (2003). Crime data mining: an overview and case studies. In. *Proceedings of the 2003 annual national conference on Digital government research* (pp. 1-5). Texas: University of Arizona.

[3] Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., & Febriansyah, A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *JIEET (Journal of Information Engineering and Educational Technology) 2(2)* , 65-69.

[4] Fayyad, U., & Uthurusamy, R. (2002). Evolving data mining into solutions for

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

insights. *Communications of the ACM, 45(8)* , 28-31.

[5] Gendi, M., & Munteanu, C. (2021). Towards a chatbot for evidence gathering on the dark web. *In CUI 2021-3rd Conference on Conversational User Interfaces* , 1-3.

[6] Kuk, K., Stanojević, A., Jovanović, M., & Nedeljković, S. (2018). Intelligent e-service for detecting malicious code based agent technology. *Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics*, (pp. 1-6).

[7] Laranjo, L., Dunn, A. G., Tong, H. L., Kocaballi, A. B., Chen, J., Bashir, R., et al. (2018). Conversational agents in healthcare: a systematic review. *Journal of the American Medical Informatics Association, 25(9)* , 1248-1258.

[8] Marufah, N., Rahmat, H. K., & Widana, I. D. (2020). Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7(1)* , 191-201.

[9] Mashabi, S. (2021, Sep 14). *BSSN: Hingga Agustus 2021 Tercatat 888 Juta Serangan Siber*. Retrieved Okt 27, 2021, from kompas.com: https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber

[10] Nahwan, D., Nurhayani, N., Nugroho, I. S., & Srimurni, R. R. (2021). Analisa Manajemen Strategis Program Pelatihan SDM TIK Polri dalam Menghadapi Kejahatan Siber Era 4.0. *Media Nusantara, 18(2)* , 133-144.

[11] Noviantini, N., Remaja, I. N., & Mariadi, N. N. (2021). Efektivitas Patroli Siber Dalam Mengungkap Kasus Ujaran Kebencian Di Wilayah Hukum Polres Buleleng. *Kertha Widya, 9(1)* , 28-51.

[12] Piscopo, A., Siebes, R., & Hardman, L. (2017). Predicting sense of community and participation by applying machine learning to open government data. *Policy & Internet, 9(1)* , 55-75.

[13] Rachmadie, D. T. (2020). Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016. *Jurnal Hukum Pidana dan penanggulangan Kejahatan, 9(2)* , 128-156.

[14] Radulov, N. (2019). Artificial intelligence and security Security 4.0. *Security & Future, 3(1),* , 3-5.

[15] Schachner, T., Keller, R., & Von Wangenheim, F. (2020). Artificial intelligence-based conversational agents for chronic conditions: systematic literature review. *Journal of medical Internet research, 22(9)* , e20701.

[16] Sivčević, D., Košanin, I., Nedeljković, S., Nikolić, V., Kuk, K., & Nogo, S. (2020). Possibilities of used intelligence based agents in instant messaging on e-government services. *2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-5). IEEE.

[17] Stănilă, L. (2020). Memories Of The Future-Sweetie And The Impact Of The New Technologies On The Criminal Justice System. *EU and comparative law issues and challenges series (ECLIC), 4* , 557-575.

[18] Zed, M. (2003). *Metode Penelitian Kepustakaan.* Jakarta : Yayasan Obor Indonesia.

HALAMAN INI SENGAJA DIKOSONGKAN

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)