Triwikrama: Jurnal Ilmu Sosial
Volume 8 No. 10 Tahun 2025
E-ISSN: 2988-1986
Open Access:

PERAN *ARTIFICIAL INTELLIGENCE* DALAM MENCEGAH DAN MENINGKATKAN KEAMANAN SIBER SUATU NEGARA (MENILITIK STUDI KASUS WEB BRI)

Wahyu Putra Ramadhan[1], Wira Atman[2]
[1,2]Fakultas Ilmu Sosial dan Politik, Departemen Ilmu Hubungan Internasional
Universitas Hasanuddin, Makassar, Indonesia

ARTICLE INFO

Article history:
Received: June 2025
Revised: June 2025
Accepted: June 2025
Available online

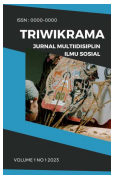
Korespondensi: Email:
[1]Wahyuputraramadhan08@gmail.com,
[2]Atmannyawiraaa@gmail.com

Abstrak

Artificial intelligence atau kerap di sebut AI merupakan teknologi dimana komputer memungkinkan mengerjakan dan melakukan tugas-tugas yang biasanya dilakukan manusia dan memerlukan keterampilan dan kecerdasan tertentu dan bisa beradaptasi pada situasi tertentu. *Artificial intelligence* di jaman sekarang ini sangat membantu pekerjaan manusia, baik dalam membantu mencari dan memberi penjelasan mengenai hal tertentu hingga kepada penjagaan keamanan siber yaitu data. Cara kerja dari AI itu sendiri menurut penulis melibatkan beberapa disiplin seperti *searching machine* dan juga *deep learning* yang dimana komputer memungkinkan melakukan analisis terhadap hal-hal yang diberikan dan juga mengidentifikasi pola dan juga memprediksi hal-hal atau tindakan tertentu. yang akan penulis bahas adalah mengenai *phising*, yang dimana *phising* adalah metode yang digunakan aktor menggunakan teknik rekayasa sosial untuk menyamar sebagai entitas yang dianggap sah dan dapat mengakses hingga mencuri informasi pribadi tanpa izin. Di zaman yang serba canggih dan serba digital ini, Ada banyak sekali terobosan-terobosan baru yang ditemukan dan sangat bermanfaat bagi kemudahan pekerjaan manusia, Salah satu yang sangat memberikan dampak besar ialah *Artificial intelligence* yang hingga sekarang ini hampir menyentuh segala aspek kehidupan termasuk aspek keamanan. Keamanan data suatu negara merupakan hal yang sangat penting untuk itu diperlukan upaya-upaya untuk mencegah terjadinya *cryber crime* yang bisa datang dari mana saja, Mulai dari aktor negara itu sendiri hingga aktor luar negara bahkan aktor non negara. Dalam tulisan ini membahas mengenai web bank BRI yang dipalsukan (*phising*) oleh pihak yang tidak bertanggung jawab. Bocornya data korban menyebabkan membuat para nasabah kehilangan kepercayaan terhadap perusahaan tersebut masa itu. Peran *Artificial Intelligence* untuk mencegah hal-hal tersebut yang akan di bahas dalam tulisan ini, bagaimana konsep dari *Artificial intelligence* dalam sektor keamanan.

Kata kunci: *Artificial Intelligence, cyber crime, phising.*

Triwikrama: Jurnal Ilmu Sosial
Volume 8 No. 10 Tahun 2025
E-ISSN: 2988-1986
Open Access:



PENDAHULUAN

Latar Belakang

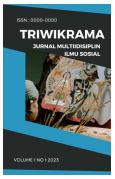
Tulisan ini akan membahas tentang tulisan ini dengan memberikan penjelasan mendasar seperti apa itu keamanan siber, mengapa keamanan siber itu penting bagi suatu negara, konsep *artificial intelligence*, Hal-hal tersebut yang akan penulis jelaskan pada bab pertama ini. keamanan siber merupakan rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak/*hardware & software)*, terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber digunakan sebagai wadah untuk melindungi *big data* dan bentuk pencegahan terhadap kerusakan data yang tidak di inginkan. Dengan definisi lain keamanan siber merupakan segala cara atau semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan dari ketersediaan dan kerahasiaan dari sebuah informasi yang di lakukan oleh *threat actor*. Keamanan siber penting bagi suatu negara untuk melindungi data-data penting, jaringan, dan sistem komputer negara, bahkan di Indonesia sendiri terdapat lembaga yang memiliki fokus terkait hal tersebut, yaitu Kementerian Komunikasi dan Digital atau KOMDIGI dan juga tugas menyelidiki kejahatan siber sudah menjadi tugas dan fungsi unit kejahatan siber (*cyber crime*) mabes polri di Indonesia. pertahanan negara dari sisi siber (*cyber defence*) menjadi ranahnya Kementerian Pertahanan (Kemhan), yang mana saat ini sudah memiliki Pusat Operasi Siber (*Cyber Operation Center*).

Keamanan siber sangat krusial bagi suatu negara karena berkaitan dengan perlindungan data penting, infrastruktur kritis (energi, transportasi, dan komunikasi), serta kepercayaan publik terhadap pemerintah dan lembaga negara. Serangan siber sendiri dapat menyebabkan kerusakan sistem, kehilangan data, gangguan layanan, bahkan ancaman terhadap keamanan suatu negara. Hal ini sangatlah sensitif mengingat perkembangan zaman dan penggunaan teknologi yang sudah sangat maju tidak dapat dipungkiri pasti ada saja pihak yang menggunakannya untuk hal yang tidak sepatutnya. Maka dari itu kesadaran masyarakat dalam suatu negara harus ditingkatkan agar hal-hal yang tidak diinginkan tidak terjadi di masa yang akan datang.

Kasus yang ingin di angkat pada pembahasan kali ini adalah situs web palsu clickbri.com, dimana pada kasus yang terjadi pada tahun 2022 ini mengalami kerugian pribadi sebesar 1,1 Miliar rupiah. Pembobolan yang dilakukan pelaku terhadap korban bisa terjadi karena korban masuk ke dalam *link* yang diberikan pelaku, setelah itu korban merasa bahwa web atau *link* yang dibuat oleh pelaku ini sangat meyakinkan dimana korban tentu saja berani untuk memberikan *password* dan juga *username*-nya. Alhasil pelaku tentu saja bisa menguras habis isi rekening korban dan pembobolan baru diketahui korban ketika mendapatkan informasi melalui *whatsapp* tentang perubahan biaya transfer.

KAJIAN TEORITIS

Cyber crime merupakan salah satu jenis kejahatan internasional kontemporer, maksud dari kontemporer ialah kejahatan jenis ini salah satu yang berkembang pesat, yang berawal pada periode 1970an dan terus berkembang hingga hari ini. Dalam perkembangannya yang sangat pesat dengan modus yang beragam, maksudnya ialah melibatkan bukan hanya pelaku dalam konteks individu namun pelaku juga dapat melibatkan negara sebagai aktor intelektual. Dari studi kasus yang di telah di jelaskan di atas tindakan kriminal tersebut bisa di kategorikan *cyber crime* dalam dunia ilmu hubungan internasional. Dalam ilmu hubungan internasional sendiri kejahatan yang berbasis dunia maya seperti ini dapat mengancam integritas suatu negara karena dapat menyebabkan bocor nya data penting dari suatu negara. Menurut *United*



States Departement of Justice, cyber crime merupakan tindakan ilegal apapun yang memerlukan pengetahuan tentang teknologi komputer untuk perbuatan jahat, penyidikan, atau penuntutan.

Menurut freddy haris SH. MH. LLM. yaitu dosen terkemuka dari universitas Indonesia mengemukakan definisi dari *cyber crime* yaitu tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama, dan juga merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. Adapun karakteristiknya yaitu *Unauthorized acces*, dengan maksud untuk memfasilitasi kejahatan, *Destruction of* data, yang dimana pelaku dapat membobol data penting dan menggunakannya dengan maksud tertentu, *Easy to acces*, dengan maksud para calon korban gampang untuk mendapatkan portal-portal yang dibuat oleh para pelaku.

Dari definisi di atas tentu pelaku kejahatan *cyber crime* ini melakukannya jarak jauh dan juga dari studi kasus yang sudah di bahas ada beberapa aktor yang melakukannya untuk menguntungkan diri sendiri. Tentu saja para pelaku *cyber crime* ini memiliki kepintaran di atas rata-rata mengenai informasi teknologi.

METODE PENELITIAN

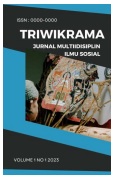
Tulisan ini menggunakan penelitian metode kualitatif deskriptif yang dimana pendekatan penelitian yang dilakukan ialah menggambarkan fenomena, peristiwa atau situasi tertentu secara spesifik dan menyeluruh, dengan fokus pada pemahaman makna dan konteks sosialnya. Penelitian dengan metode ini juga bertujuan untuk memberikan pemahaman yang kaya dan detail tentang suatu hal, misalnya saja bagaimana *artificial intelligence* dalam mencegah terjadinya serangan siber seperti *phising,* dan juga memberikan penjelasan lebih dalam dari cara kerja serang siber itu sendiri.

konsep serangan siber dalam ilmu hubungan internasional sendiri sudah lama dikenal dan telah menjadi isu global bagi beberapa negara, Apa lagi isu mengenai serangan siber sangatlah berpengaruh pada keamanan nasional masing-masing negara. Dengan adanya pengetahuan mengenai keamanan siber, negara-negara dapat dengan mudah mencegahnya apa lagi dengan munculnya *artificial intelligence* yang dapat membantu pencegahan dengan skala *real-time*.

HASIL DAN PEMBAHASAN

Studi kasus yang akan penulis bahas adalah mengenai *phising,* yang dimana *phising* adalah metode yang digunakan aktor menggunakan teknik rekayasa sosial untuk menyamar sebagai entitas yang dianggap sah dan dapat mengakses hingga mencuri informasi pribadi tanpa izin. *Phising* bisa di kategorikan sebagai tindakan kriminal karena aktor atau pelaku dapat mengakses data korban dan mengambil seperti contohnya mungkin sejumlah uang yang ada di rekening korban. Pada tahun 2022-2023 kasus *phising* sangat marak terjadi 50 persen dari kasus tersebut ialah mengenai lembaga keuangan. *Phising* mengandalkan *website* palsu yang dibuat sedemikian rupa hingga tampilannya dapat meyakinkan korban, sehingga korban berani untuk menggunakan dan memasukkan *username* dan *password* pada *website* yang dibuat oleh pelaku.

Pada tahun 2024 saja kerugian finansial di dunia akibat insiden *phising* mencapai angka 150.000 US dollar (2 triliun lebih) berdasarkan informasi BEC atau *Business Email Compromise*. *Phising* tidak hanya merugikan secara finansial tetapi juga bagi pihak perusahaan karena hilangnya kepercayaan masyarakat terhadap produknya. Perkembangan ilmu pengetahuan dan teknologi, khususnya teknologi informasi sudah terbukti banyak memberi dampak positif bagi semua sektor baik dari pendidikan, militer hingga industri. Tetapi di balik dampak positif tersebut selalu saja timbul tantangan baru dan ada beberapa pihak yang tidak bertanggung



jawab dan banyak mengambil kesempatan untuk mendapatkan keuntungan dengan cara *phising*.

Adapun penjelasan sederhana mengenai cara kerja dari *phising* itu sendiri, *phishing* dilakukan untuk memancing korban ke dalam jebakan seorang *phisher*. *Phishing* merupakan aktivitas seorang *phisher* untuk mendapatkan informasi pribadi seseorang pengguna pada saat pengguna menggunakan web palsu yang terlihat seperti tampilan asli atau resmi dari situs web sebenarnya. Untuk mengelabui pengguna seorang *phisher* menggunakan *pop-up*, email, spanduk agar pengguna terpancing ke dalam jebakan seorang *phisher* agar memberikan informasi pribadi dalam web palsu tersebut. Di situlah para *phisher* memanfaatkan kelalaian pengguna untuk mendapatkan informasi pribadinya.

Dampak yang dirasakan oleh korban pada kasus ini ialah bocornya data pribadi dan juga akses *login* pada web, di samping itu juga banyak nya pelanggan pengguna bank BRI yang kehilangan kepercayaan setelah kasus ini, takutnya mereka akan merasakan hal yang sama akibat keamanan yang mungkin kurang setelah kasus ini terjadi. Namun kasus ini telah laporkan dan ditangani oleh Direktorat Reserse Kriminal Khusus Polda Sumatera Barat dan pelaku di kenai hukuman pidana pada pasal 378 KUHP.

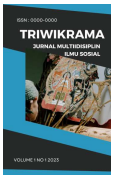
Phising sendiri pada dasarnya bagian dari kejahatan siber (dalam ilmu hubungan internasional disebut *cyber crime*), yang memiliki dampak lintas batas negara, sehingga menjadi isu keamanan yang bersifat global. Serangan *phising* tidak hanya merugikan individu dan perusahaan secara finansial, tetapi juga dapat mengancam stabilitas ekonomi dan keamanan nasional suatu negara, terutama jika menyerang infrastruktur atau data penting dari suatu lembaga pemerintahan negara tertentu. Oleh karena itu keamanan siber menjadi bagian dari agenda keamanan internasional yang membutuhkan kerjasama bilateral maupun multilateral dan harus dicegah sedini mungkin.

Dalam konteks ilmu hubungan internasional, negara memiliki tanggung jawab untuk melindungi warganya dari ancaman siber, termasuk *phising* ini, dengan mengembangkan kebijakan keamanan siber yang efektif dan regulasi yang ketat terhadap lembaga keuangan sesuai dengan studi kasus yang di angkat. Bank BRI sebagai BUMN juga harus berbenah diri dan meningkatkan keamanan sistem digitalnya agar tetap dapat menjaga kepercayaan masyarakat dan nasabahnya, yang dimana jika hilang akan sangat berdampak pada keberlanjutan lembaga dan juga tentunya stabilitas ekonomi nasional dan citra negara Indonesia di mata internasional.

Adapun implikasi politik dimana kerugian finansial yang besar akibat dari *phising* seperti yang dijelaskan pada studi kasus dapat mempengaruhi kepercayaan investor dan stabilitas ekonomi suatu negara. Dalam konteks hubungan internasional, Hal ini sangat mempengaruhi posisi negara dalam ekonomi global dan hubungan bilateral dengan negara lain, Terutama dalam hal investasi dan kerjasama teknologi.

KESIMPULAN

Di zaman sekarang ini *Artificial Intelligence* selain membantu memudahkan beberapa sektor seperti pendidikan membantu mencari materi dan memahami beberapa hal, komunikasi membantu memberikan pemahaman tentang bahasa dan juga penggunaan teknologi hingga memudahkan pekerjaan yang cukup kompleks sekalipun. Dalam konteks keamanan siber AI sendiri dapat menjadi salah satu solusi yang berpotensi karena AI dapat meningkat kemampuan deteksi, respons dan mitigasi ancaman siber secara signifikan. AI memungkinkan identifikasi pola ancaman dan prediksi serangan siber sebelum terjadi, memungkin para korban untuk bisa lebih terbuka dan memahami ancaman penyerangan keamanan siber. AI juga dapat memproses



data dari berbagai sumber, memungkinkan tindakan pencegahan *real time* dan deteksi serta respons otomatis terhadap ancaman serangan siber.

AI sendiri dapat memberikan fitur seperti *machine learning* yang dimana AI dapat menganalisis data besar secara *real-time* dan mengidentifikasi pola yang menunjukkan aktivitas mencurigakan atau berbahaya. Sebagai contoh saja dalam kehidupan menggunakan sosial media setiap hari dimana *log in* aktivitas jaringan untuk mendeteksi anomali atau orang tidak di kenali yang terindikasi atau berpotensi melakukan serangan peretasan akun. Dengan kemampuan prediksi yang semakin baik, deteksi *malware* berbasis AI menjadi semakin efektif untuk di cegah dan di tangani sehingga ancaman keamanan siber dapat di hentikan.

Kemampuan AI sendiri juga untuk mendukung evaluasi keamanan dan manajemen risiko juga sangatlah membantu dan signifikan, dimana AI dapat membantu untuk secara otomatis mengevaluasi kerentanan sistem dan memberikan rekomendasi perbaikan sistem agar ancaman keamanan siber di masa depan dapat di hindari dan di cegah. Dalam penggunaan teknologi yang kompleks dan juga terus berkembang cara seperti ini dapat digunakan oleh para pihak pemegang data-data penting seperti pemerintahan agar mereka dapat menyesuaikan strategi mereka dengan cepat untuk menghadapi ancaman baru terhadap keamanan siber. Pendekatan seperti ini mendukung ketahanan jangka panjang dan memastikan para pelaku pemerintahan atau mungkin organisasi yang memiliki data penting bahkan kepentingan individu selalu bisa berada selangkah lebih di depan perihal ancaman siber.

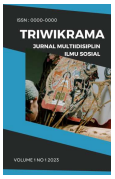
Di zaman yang serba canggih dan serba teknologi ini, kita sebagai manusia harus selalu update dengan perkembangan zaman. Bukan berarti kita bergantung pada teknologi yang ada namun kita harus menggunakan teknologi tersebut sebaik-baik mungkin bukan justru menjadikannya alat untuk melakukan kejahatan seperti kasus-kasus *cyber crime* yang telah paparkan di atas. Selanjutnya sebagai anak yang sedang mempelajari ilmu hubungan internasional, melihat sebuah fenomena menggunakan paradigma yang telah di pelajari sangat membantu untuk menganalisis fenomena yang tengah di kaji. Sebagai contoh saja untuk melihat fenomena peretasan ini menggunakan paradigma atau kacamata ilmu hubungan internasional yaitu *cyber crime* penulis dapat menganalisis maksud dan tujuan, tata cara, dan juga dampak dari fenomena tersebut dengan baik dan benar.

Dari kasus yang di angkat, penting nya untuk masyarakat untuk selalu bisa *update* dengan berita atau teknologi yang terbarukan, karena hal tersebut dapat membuat kita paham algoritma baru yang ada didunia. Semisal saja *Artificial intelligence* yang akan mampu memudahkan kita untuk mengerjakan sesuatu, namun tidak sampai situ saja pastinya, ke depannya pasti ada saja orang-orang yang akan menggunakan AI untuk melakukan tindakan kriminal lainnya. Itu lah mengapa kita harus selalu update dan tidak ketinggalan dengan hal-hal yang berkembang di dunia ini.

DAFTAR PUSTAKA

Wibisono, G., Gultom, R. A., & Mantoro, T. (2024). “Strategi Peningkatan Kapabilitas Satuan Siber Dispamsanau Melalui Pemanfaatan Artificial Intelligence Pada Keamanan Siber Berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1”. *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, *7*(1), 968-975.

Sinaga, M. P., Ginting, E., Nurdin, M. R., & Putra, M. D. (2023). “Analisis Ancaman Phising Terhadap Layanan Online Perbankan”. *UNES Journal of Scientech Research*, *8*(1), 041-047.



Wibowo, A., Navalino, D. A., & Siagian, F. H. (2024). "STRATEGI PEMANFAATAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DALAM PERTAHANAN NEGARA GUNA MENGHADAPI ANCAMAN SIBER". *Jurnal Strategi Pertahanan Darat*, *1*(1).

Sinaga, M. P., Ginting, E., Nurdin, M. R., & Putra, M. D. (2023). "Analisis Ancaman Phising Terhadap Layanan Online Perbankan". *UNES Journal of Scientech Research*, *8*(1), 041-047.

Warsiti, T., & Markoni, M. (2023). "Perlindungan Hukum Terhadap Korban Kejahatan Cyber Berbentuk Phising Dalam Transaksi Perdagangan Internasional". *Jurnal Multidisiplin Indonesia* , *2* (6), 1109-1125.

Rohendi, A. (2015). "Perlindungan Konsumen Dalam Transaksi E-Commerce Perspektif Hukum Nasional Dan Internasional". *Jurnal Ecodemica: Jurnal Ekonomi Manajemen Dan Bisnis* , *3* (2), 474-488.

Manorek, BD (2025). "PENEGAKAN HUKUM PIDANA DALAM MEMBERANTAS KEJAHATAN PENCURIAN DATA ELEKTRONIK (PHISING)". *LEX PRIVATUM* , *15* (2).

Farid, I., Reksoprodjo, A. H., & Suhirwan, S. (2023). "Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber". *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *10*(2), 779-788.

Hermawan, A. Z., Anggoro, M. N., Lozera, D., & Faroqi, A. (2023, November). "Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (AI) Terhadap Keamanan Data di Indonesia". In *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* (Vol. 3, No. 1, pp. 581-591).

Setyawan, A. P., & Marzaman, A. P. (2025). "ARTIFICIAL INTELLEGENCE DALAM PERTAHANAN GLOBAL: TRANSFORMASI STRATEGI DAN KEAMANAN MILITER DI INDONESIA". *Triwikrama: Jurnal Ilmu Sosial*, *8*(4), 11-20.

Nur'adila, R. Tren Keamanan Menggunakan Artificial Intelligence.

Ilyas, F. Q. (2024). "Formula Model Penanganan Phising Pada Bank BRI: Analisis, Dampak, dan Implementasi", Doctoral dissertation, Universitas Hasanuddin.

Maramis, A. V. (2025). "TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DALAM MENGATASI CYBERCRIME PADA KASUS PHISHING". *LEX PRIVATUM*, *14*(5).

Suharto, M. A., & Apriyani, M. N. (2021). "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional". *Risalah Hukum*, 98-107.

Ketaren, E. (2016). "Cybercrime, cyber space, dan cyber law". *Jurnal Times*, *5*(2), 35-42.