JGC XV (1) (2026)
JURNAL GLOBAL CITIZEN
JURNAL ILMIAH KAJIAN PENDIDIKAN KEWARGANEGARAAN
http://ejurnal.unisri.ac.id/index.php/glbctz/article/view/....
Diterima : 7-5-2026 , Disetujui : 8-6-2026, Dipublikasikan: 1-7-2026

MENYIKAPI KEAMANAN SIBER BAGI WARGA NEGARA DAN PERTAHANAN NEGARA DI ERA SOCIETY 5.0

Alven Henas Orlando[1], Fatma Ulfatun Najicha[2]
[1,2]Universitas Sebelas Maret Jl. Ir. Sutami No.36, Kentingan, Jebres, Surakarta, Indonesia
alvenorlando@student.uns.ac.id[1], fatmanajicha_law@staff.uns.ac.id[2]

ABSTRAK

Dalam berkembang teknologi yang semakin maju, muncul istilah *Society* 5.0. Dalam *Society* 5.0, orang diharapkan memanfaatkan teknologi dalam setiap aspek kehidupan mereka. Dalam perkembangan teknologi yang semakin maju, muncul ancaman serangan siber yang dapat mengambil alih sistem komputer atau mengambil data secara tidak sah. Sehingga dalam menyikapi hal tersebut perlu tindakan dari masyarakat dan pemerintah. Masyarakat perlu memahami segala bentuk serangan siber dan memahami dampak serangan siber. Serta masyarkat perlu melindungi diri dari serangan siber. Tidak hanya masyarakat, pemerintah memiliki peran dalam melindungi data penduduk dan data yang bersifat sensitif lainnya. Dalam hal ini pemerintah perlu mengambil tindakan pencegahan dan memperkuat sistem keamanan siber negara.
Kata kunci : society 5.0, serangan siber, sistem keamanan siber

ABSTRACT

In the development of increasingly advanced technology, the term society 5.0 has emerged. In society 5.0, people are expected to utilize technology in every aspect of their lives. With the development of advanced technology, there is a threat of cyberattacks that can take over computer systems or retrieve data unlawfully. So in responding to this, action is needed from the community and the government. People need to understand all forms of cyberattacks and their impact. And people need to protect themselves from cyberattacks. Not only the community, the government have a role in protecting population data and other sensitive data. In this case, the government needs to take preventive measures and strengthen the country's cyber security system.
Keyword : society 5.0, cyber security, cyberattacks

PENDAHULUAN

Di era digital, istilah "kewarganegaraan digital" muncul dan dapat didefinisikan sebagai standar kebiasaan dan perilaku yang tepat saat menggunakan teknologi informasi. Hal ini berkaitan dengan orang-orang yang dapat menggunakan internet dengan rutin. Kewarganegaraan digital terdiri dari hal-hal seperti akses digital, perdangan digital, komunikasi digital, literatur, etika digital, hukum digital, hak dan kewajiban digital, kesehatan digital, dan keamanan digital. Bagian-bagian keamanan digital ini sangat

penting untuk menjaga keamanan data dan mencegah serangan malware yang dapat mengambil data pengguna.

Menurut gagasan Jepang, *Society* 5.0 bertujuan untuk memasukkan teknologi ke dalam kehidupan sehari-hari dan memungkinkan masyarakat mengakses ruang maya yang mirip dengan ruang fisik. Dengan teknologi yang semakin canggih, masyarakat 5.0 diharapkan dapat memperluas kehidupan manusia (Zulfa & Najicha, 2022). Konsep ini menggunakan teknologi seperti AI (*Artificial intelligence*) berbasis big data dan robot untuk membantu atau melakukan pekerjaan manusia. Saat ini, penggunaan teknologi sudah menjadi bagian dari kehidupan manusia. Tujuan dari konsep *Society* 5.0 adalah untuk memberikan layanan yang lebih baik kepada masyarakat dengan bantuan teknologi (Kirani & Najicha, 2022). Tidak hanya berdampak pada pelayanan masyarakat, namun teknologi akan mengakibatkan perubahan dalam interaksi sosial secara langsung maupun virtual (Yasinta & Najicha, 2022). Perkembangnya teknologi memngaruhi perilaku dan perbuatan kehidupan di masyarakat (Gunawan & Najicha, 2022). Jadi masyarakat harus tetap terbuka dan mengikuti perkembangan teknologi (Pratama & Najicha, 2022).

Namun, di balik manfaat dan potensi yang luar biasa, ada masalah yang harus diatasi. Serangan siber telah berkembang menjadi ancaman yang signifikan dalam era *Society* 5.0, memengaruhi kehidupan sehari-hari masyarakat yang terhubung secara luas dengan teknologi informasi dan komunikasi. Ketergantungan yang tinggi pada teknologi merupakan penyebab utama serangan siber di era ini. Berbagai bagian kehidupan *Society* 5.0 bergantung pada teknologi, seperti infrastruktur kota, transportasi, sistem kesehatan, dan lainnya. Ketergantungan ini memungkinkan pencuri untuk memanfaatkan celah keamanan dan menimbulkan gangguan.

Infrastruktur dan jaringan di *Society* 5.0 semakin kompleks dan saling terhubung. Serangan siber dapat mengeksploitasi kerentanan dalam sistem yang kompleks ini. Serangan DDoS yang dapat menghentikan layanan penting atau serangan ransomware yang mengenkripsi data dan meminta tebusan adalah beberapa contoh serangan yang dapat menyebabkan kerugian besar bagi *Society* 5.0. Di era yang semakin kompleks ini, penting untuk melindungi infrastruktur dan jaringan yang semakin kompleks dengan membangun keamanan siber yang tangguh dan sistem deteksi intrusi yang canggih.

Pertahanan negara menghadapi serangan siber yang semakin kompleks di era *Society* 5.0. Infrastruktur militer yang penting untuk pertahanan negara, seperti infrastruktur kritis dan sistem komunikasi militer, menjadi sasaran utama serangan. Serangan siber yang berhasil dapat mengganggu pertahanan negara dan memberikan keuntungan kepada penyerang. Dalam hal ini, menjaga infrastruktur dan sistem komunikasi sangat penting untuk memastikan bahwa pertahanan negara siap dan kuat.

Selain itu, serangan siber dapat menargetkan informasi sensitif seperti rencana militer, strategi politik, dan data intelijen. Jika data ini jatuh ke tangan orang yang salah, itu dapat menyebabkan kerugian besar dan mengancam keamanan negara. Oleh karena itu, di era *Society* 5.0, pertahanan negara harus memprioritaskan perlindungan informasi sensitif. Negara harus mengembangkan kebijakan keamanan yang kuat, mengadopsi tindakan pengamanan yang canggih, dan meningkatkan kesadaran dan pelatihan personel untuk menghadapi serangan siber yang terus-menerus dan meningkatkan kekuatan pertahanan negara.

Oleh karena itu, baik pemerintah maupun warga negara harus memberikan perhatian khusus dalam menghadapi serangan siber. Hal ini disebabkan oleh bagaimana teknologi, internet, dan berbagai aspek kehidupan saling terintegrasi secara luas. Keamanan data dan sistem di sini menjadi sangat penting. Pemerintah harus menerapkan kebijakan dan tindakan yang

kuat untuk melindungi infrastruktur negara dan data sensitif. Di sisi lain, masyarakat harus meningkatkan kesadaran tentang serangan siber, mengamankan perangkat mereka, dan mengadopsi praktik keamanan yang tepat guna. Di era *Society* 5.0, kerja sama antara pemerintah dan masyarakat akan sangat penting untuk menghadapi tantangan keamanan siber yang semakin sulit.

METODE

Penelitian ini menggunakan penelitian kepustakaan, yaitu jenis penelitian kualitatif yang biasanya dilakukan tanpa melakukan penelitian di lapangan untuk mengumpulkan data. Penelitian kepustakaan memeriksa berbagai sumber teks yang berkaitan dengan topik jurnal yang diteliti. Dalam konteks ini, penelitian ini hanya didasarkan pada karya – karya tulis. Membaca artikel, buku, koran, dan laporan yang terkait topik penelitian adalah cara untuk mendapatkan informasi.

PEMBAHASAN

Serangan Siber

Serangan siber serangkaian tindakan yang dilakukan oleh pihak yang tidak berwenang atau jahat dengan tujuan merusak, mengambil alih, atau mencuri informasi dari sistem komputer. Tindakan ini dapat meliputi pembobolan keamanan, penyebaran malware, serangan DDoS, pencurian identitas, atau manipulasi data. Serangan siber terjadi melalui jaringan internet atau sistem komputer yang terhubung (Herdiana et al., 2021). Penyerang memanfaatkan celah keamanan yang ada pada infrastruktur jaringan atau perangkat lunak yang digunakan, baik pada tingkat individu maupun organisasi. Penyerang dapat menggunakan teknik – teknik canggih, seperti phising, peretasan password, atau serangan berbasis sosial untuk mendapatkan akses yang tidak sah.

Serangan siber adalah bahaya yang dapat berdampak besar pada orang dan organisasi. Serangan tersebut dapat menyebabkan kehilangan kepercayaan pelanggan dan kerusakan reputasi, serta menyebarluaskan data pribadi. Langkah-langkah keamanan yang kuat harus diambil untuk melindungi diri dari serangan siber yang terus berkembang. Ini termasuk menginstal perangkat lunak antivirus terbaru untuk mendeteksi dan mencegah infeksi *malware*, mengamankan jaringan dengan *firewall* yang dapat mencegah akses yang tidak sah, dan melakukan pembaruan sistem rutin untuk memperbaiki kerentanan yang mungkin dieksploitasi oleh penyerang.

Serangan siber tidak terbatas pada individu atau kelompok tertentu; sistem pertahanan negara juga dapat terkena dampak. Serangan siber, dalam konteks pertahanan negara, adalah upaya yang disengaja dan terorganisir yang dilakukan oleh negara atau entitas yang berhubungan dengan negara untuk mencapai berbagai tujuan. Beberapa contoh serangan jenis ini termasuk pengumpulan intelijen untuk kepentingan militer atau politik, spionase untuk mendapatkan informasi rahasia. Spionase dilakukan dengan menyadap alat komunikasi atau jaringan komunikasi melalui internet (Adrian, 2022). Sabotase untuk merusak atau menghancurkan infrastruktur atau sistem komunikasi negara lain yang penting, atau pengganggguan sistem kritis yang dapat menyebabkan kerugian besar. Serangan siber negara dapat mengancam stabilitas dan keamanan suatu negara serta hubungan internasional.

Serangan siber sangat memengaruhi kehidupan masyarakat modern. Serangan ini dapat menyebabkan kehilangan data pribadi, kerugian finansial, gangguan layanan publik, pencurian properti intelektual, penyebaran desinformasi, gangguan privasi dan keamanan digital, dan kehilangan reputasi. Pemerintah dan sektor swasta harus bekerja sama untuk melindungi masyarakat dengan kebijakan, pelatihan, dan infrastruktur keamanan yang memadai. Di sisi lain, masyarakat harus meningkatkan kesadaran tentang ancaman serangan siber dan mengambil langkah-langkah perlindungan yang tepat.

Bentuk Serangan Siber

Model kejahatan siber memiliki banyak jenis karena kemajuan teknologi. Serangan siber termasuk hacking, penipuan (*phishing*), manipulasi program (bajakan), dan pencurian data (Hanafi, 2021). Terdapat tiga kelompok jenis ancaman: ancaman perangkat keras (ancaman *hardware*), ancaman perangkat lunak (ancaman *software*), dan ancaman data/informasi (Rizki, 2022). Serangan siber juga mencakup serangan DDoS, serangan *malware*, dan serangan *Man in the Middle* (MitM). Namun, serangan yang sering terjadi di pemerintahan dan masyarakat adalah penipuan, juga dikenal sebagai *phishing*, dan pencurian data.

Serangan *phishing* menggunakan email dan situs web palsu untuk mendapatkan data pengguna sensitif (DM et al., 2022). Serangan phishing terjadi ketika pelaku berpura-pura menjadi organisasi resmi, seperti bank atau perusahaan, dengan mengirimkan email atau mengarahkan pengguna ke situs website palsu yang mirip dengan situs web aslinya. Mereka menggunakan pesan yang mendesak, ancaman, atau hadiah untuk membuat korban mengungkapkan informasi pribadi penting. Penyerang dapat mencuri identitas, melakukan penipuan finansial, atau mengakses akun penting korban jika korban terjebak dan memberikan data sensitif. Serangan *phishing* dapat mengakibatkan kerugian moneter yang signifikan, kerugian privasi, dan kerusakan reputasi dan kepercayaan individu atau perusahaan yang disasar. Untuk melindungi diri dari ancaman ini, sangat penting untuk memahami teknik serangan dan tetap waspada terhadap email atau tautan mencurigakan.

Serangan *malware* dilakukan dengan memasukkan perangkat lunak jahat ke sistem komputer target. *Spyware*, virus, *worm*, *trojan*, dan *ransomware* adalah beberapa jenis *malware* yang paling umum. Virus dapat mereplikasi diri dan menyebabkan kerusakan pada sistem. *Worms* dapat menyebar melalui jaringan dan menginfeksi banyak sistem. Meskipun terlihat seperti perangkat lunak yang bermanfaat atau menyenangkan, trojan sebenarnya memberikan akses tak sah kepada penyerang. *Ransomware* mengenkripsi data korban dan meminta uang sebagai imbalan untuk memulihkan data. *Spyware* mengumpulkan data informasi pribadi tanpa diketahui pengguna. Data yang telah terakam akan dijual kepada individua tau perusahaan yang akan mengirimkan iklan atau menyebarkan virus (Rahmawati, 2017). Serangan *malware* ini memiliki kemampuan untuk merusak sistem, mencuri data, dan memperoleh akses sistem secara tidak sah.

Serangan DDoS (*Distributed Denial-of-Service*) adalah serangan yang bertujuan untuk membanjiri sistem target dengan lalu lintas internet yang besar, sehingga pengguna yang sah tidak dapat mengakses layanan yang dituju. Untuk melakukan serangan ini, penyerang menggunakan jaringan komputer yang diretas atau dikendalikan, yang disebut sebagai botnet, untuk mengirimkan sejumlah besar permintaan atau paket data yang tidak relevan secara bersamaan. Serangan ini dapat menyebabkan masalah pada sistem, layanan, atau bahkan membuat layanan sepenuhnya tidak dapat diakses oleh pengguna yang berwenang. Selain itu, serangan DDos ini dapat menyebabkan server mati dan tidak dapat beroperasi lagi, sehingga server tidak dapat memberikan layanan secara otomatis(Dwiyatno et al., 2019).

Serangan MitM *(Man in the Middle Attack*) adalah suatu teknik jenis serangan yg dapat memposisikan dirinya pada antara percakapan yaitu dialog antara ke 2 belah pihak mirip model user serta *website* (Diansyah et al., 2023). Hal ini terjadi ketika seseorang yang berniat jahat mengganggu komunikasi antara dua entitas yang sedang berkomunikasi. Seorang penyerang dapat memata-matai, mencuri, atau memanipulasi data dalam komunikasi yang sedang berlangsung. Serangan MitM biasanya terjadi di jaringan Wi-Fi publik yang tidak aman atau melalui serangan pada protokol

komunikasi yang rentan. Penyerang dapat mengakses data sensitif seperti kata sandi, informasi keuangan, atau data pribadi. Serangan MitM membahayakan privasi dan keamanan data pengguna serta integritas komunikasi.

Serangan APT (*Advanced Persistent Threat*) adalah serangan siber yang kompleks dan berkelanjutan yang dilakukan oleh kelompok yang sangat terlatih dengan tujuan memperoleh akses ilegal ke sistem atau jaringan target untuk mencuri informasi rahasia atau mengganggu operasional. Infiltrasi, survei, dan pengintaian adalah langkah-langkah yang digunakan dalam serangan ini, selain memperoleh kontrol dan mempertahankan akses yang diperoleh secara tersembunyi. Teknik canggih digunakan oleh penyerang untuk menyembunyikan jejak dan menjaga akses yang mereka peroleh. Untuk melindungi diri dari serangan APT, deteksi dini, respons cepat, dan sistem keamanan yang kuat sangat penting.

Serangan siber jenis *Cyber-Physical Attacks* melibatkan manipulasi atau pengrusakan perangkat fisik yang terhubung ke jaringan, sehingga dapat mempengaruhi infrastruktur penting seperti sistem kontrol industri, jaringan transportasi, atau peralatan militer. Serangan ini dapat mencakup penghentian pasokan listrik, penghancuran perangkat keras, atau pengambilalihan kontrol sistem fisik melalui jaringan. Serangan jenis ini dapat mengganggu operasional, menyebabkan kerusakan fisik, atau bahkan membahayakan keselamatan dan keamanan manusia.

Menghadapi Serangan Siber

Keamanan data pribadi dan serangan siber menjadi masalah yang semakin penting di era *Society* 5.0, di mana penggunaan teknologi semakin meningkat. Perlindungan sistem dan informasi pribadi dari serangan siber telah menjadi sangat penting karena masyarakat digital semakin terhubung. Untuk menghadapi masalah ini, diperlukan tindakan proaktif untuk memastikan keamanan data, meningkatkan kesadaran akan risiko siber, dan mengembangkan solusi inovatif untuk melindungi individu dan organisasi dari serangan yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data. Hanya dengan upaya yang berkelanjutan dan kolaboratif kita dapat memastikan bahwa teknologi modern dan kemajuan dari *Society* 5.0 dapat digunakan dengan aman dan bertujuan. Kesadaran pemerintah dan masyarkat diperlukan untuk meningkatkan keamanan dari serangan siber.

a. Pemerintah

Dalam konteks meningkatkan keamanan, pemerintah harus berperan aktif dalam meningkatkan kesadaran masyarakat tentang bentuk dari serangan siber yang dapat menyerang setiap orang. Hal ini dapat dilakukan melalui kampanye kesadaran, program pelatihan, atau penyediaan sumber daya pendidikan yang relevan. Dengan meningkatkan pemahaman masyarakat tentang serangan siber, masyarakat dapat mengambil langkah – langkah yang tepat untuk melindungi diri dan mencegah serangan siber terjadi.

Selain memberikan pemahamanan kepada masyarakat, pemerintah juga perlu membangun infrastruktur yang memadai untuk memperkuat sistem keamanan negara. Hal ini mencakup investasi dalam infrastruktur keamanan yang canggih, seperti enkripsi yang kuat dan infrastruktur jaringan yang aman. Keamanan pada bidang siber ini tidak kalah pentingnya dengan keamanan dalam militer. Pemerintah perlu memberikan perhatian lebih lagi pada infrastruktur keamanan siber. Dengan memperkuat sistem keamanan data, pemerintah memberikan perlindungan yang lebih baik terhadap data identitas penduduk, data pajak, bahkan data

negara yang bersifat rahasia dari ancaman pencurian atau penyalahgunaan data. Sehingga dapat memperkuat pertahanan negara dari serangan siber dari individua atau negara lain.

Pemerintah juga perlu membentuk tim keamanan siber yang menangani serangan siber yang terjadi. Tim ini, yang terdiri dari para ahli keamanan siber, memiliki kemampuan untuk melacak dan menangani serangan siber secara efektif. Mereka secara proaktif menganalisis ancaman yang muncul, baik yang baru maupun yang sudah ada, untuk mengidentifikasi celah keamanan dan mengembangkan solusi yang tepat guna. Selain itu, tim ini juga memiliki peran penting dalam memberikan saran teknis kepada organisasi dan masyarakat umum terkait praktik keamanan siber yang optimal. Dengan pengetahuan dan keterampilan mereka, tim ini berperan dalam menjaga keamanan sistem, melindungi data sensitif, dan memberikan perlindungan yang diperlukan untuk menjaga integritas dan kerahasiaan informasi di era digital ini.

Pemerintah bertanggung jawab untuk mengembangkan kebijakan dan regulasi terkait keamanan siber. Serta menindak pelaku seperti memberikan sanksi atau pidana sesuai dengan pelanggaran yang sudah dilakukan (Gusti et al., 2020). Karena perlindungan data pribadi sebagai hak privasi semua orang sangat dipengaruhi oleh perkembangan lingkungan, seperti kemajuan teknologi informasi dan inovasi bisnis, kebijakan perlindungan data pribadi harus selalu berubah dan antisipatif (Hendra Wicaksana et al., 2020). Tidak hanya itu, suatu negara dapat dilumpuhkan dan dihancurkan dengan perang teknologi (Rahmawati, 2017). Kebijakan dan regulasi ini mencakup penetapan standar keamanan, perlindungan data, privasi, dan tindakan yang diharapkan dari organisasi dan individu dalam melindungi sistem dan informasi. Kebijakan dan regulasi yang jelas dan kuat dapat memberikan kerangka kerja yang diperlukan bagi masyarakat dan sektor swasta dalam melindungi diri mereka dari serangan siber.

b. Masyarakat

Di era *society* 5.0, di mana teknologi semakin terintegrasi dalam berbagai aspek kehidupan, menjadi sangat penting bagi masyarakat untuk mengantisipasi serangan siber. Serangan siber dapat membahayakan individu, kelompok, dan bahkan infrastruktur masyarakat yang penting. Oleh karena itu, sangat penting bagi masyarakat untuk menyadari bahwa serangan siber dapat terjadi di berbagai tempat, seperti rumah, tempat kerja, atau saat menggunakan perangkat mobile. Serangan phishing yang mencuri data pribadi, serangan malware yang merusak sistem, atau serangan ransomware yang mengenkripsi data adalah beberapa contoh serangan siber. Akibatnya, penting bagi setiap orang untuk memahami bahaya serangan siber dan mengambil tindakan yang diperlukan untuk melindungi data dan perangkat komputer mereka.

Langkah-langkah yang harus diambil oleh masyarakat untuk melindungi diri dari serangan siber termasuk penggunaan perangkat lunak keamanan yang baik, seperti antivirus dan *firewall*, untuk mencegah berbagai ancaman. Selain itu, memperbarui perangkat lunak (*software*) dan

sistem operasi dengan *patch* keamanan terbaru sangat penting untuk memperbaiki masalah keamanan yang terdahulu. Selain itu, masyarakat diharapkan tidak meng-*instal software* atau aplikasi modifikasi atau bajakan. Karena *software* bajakan tersebut sering disusupi *malware* yang dapat mengakses privasi seperti kamera, *microphone*, bahkan data pengguna.

Selain itu, sangat penting bagi masyarakat untuk menggunakan kata sandi yang kuat dan unik untuk setiap akun *email* yang digunakan untuk berbagai tujuan, seperti akun email untuk media sosial, belanja *online*, atau perbankan. Ketika Anda membuat kata sandi, Anda harus memastikan bahwa itu terdiri dari kombinasi huruf, angka, dan simbol. penggunaan kata sandi yang berbeda sehingga peretas tidak dapat menebak kata sandi Selain itu, autentifikasi dua faktor akan melindungi akun penting. Selain itu, mengubah kata sandi secara teratur dapat membantu melindungi akun dari peretas.

Selain itu, masyarakat harus berhati-hati saat menerima link atau aplikasi yang mencurigakan. Peretas dapat menggunakan tautan yang mencurigakan, seperti tautan *phishing* atau tautan yang mengarahkan ke situs berbahaya, untuk mencuri informasi pribadi atau menginstal *malware*. Aplikasi palsu juga merupakan ancaman, karena penjahat membuat aplikasi yang terlihat seperti asli tetapi sebenarnya mengandung malware atau program berbahaya lainnya. Dengan tetap waspada dan berhati-hati, kita dapat melindungi diri kita dari bahaya yang mungkin muncul saat kita mengakses internet dan menggunakan perangkat digital.

Masyarakat harus memahami pentingnya melakukan backup data secara teratur juga. Dengan memiliki salinan data yang aman, baik di *cloud* yang terenkripsi atau perangkat keras eksternal yang tidak terhubung secara terus-menerus ke jaringan, masyarakat dapat mengurangi dampak serangan *ransomware*, kegagalan perangkat keras, atau insiden lainnya. Backup data yang teratur memastikan bahwa data penting dapat dipulihkan dengan cepat dan efisien, sehingga masyarakat tidak hanya dapat melindungi data mereka tetapi juga menjaga kelangsungan operasional dan kehidupan sehari-hari yang lancar.

SIMPULAN

Pemerintah harus memberikan infrastruktur yang memadai untuk memperkuat sistem keamanan negara untuk menghadapi serangan siber di era *Society* 5.0. Ini akan memungkinkan mereka untuk memperkuat pertahanan negara terhadap serangan siber seperti sepionase, sabotase, dan serangan lainnya yang mengancam pertahanan negara. Sebaliknya, data—data penduduk dapat dilindungi dari pencurian, dan pemerintah harus menetapkan kebijakan dan regulasi terkait keamanan siber. Pemerintah dan masyarakat harus memahami jenis serangan siber yang sering terjadi. Oleh karena itu, orang-orang harus berhati-hati terhadap modus-modus penipuan dan menghindari membuka website atau menginstal aplikasi yang tidak diinginkan. karena peretas dapat mengambil data dan mengambil sistem komputer pengguna atau korban.

DAFTAR PUSTAKA

Adrian, W. (2022). POTENSI SPIONASE TERHADAP PENGGUNAAN WHATSAPP DALAM BIDANG PERTAHANAN INDONESIA.

Peperangan Asimetris (PA), *8*(2), 44–68. https://doi.org/10.33172/PA.V8I2.1454

Diansyah, T. M., Faisal, I., & Siregar, D. (2023). Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack. *Kesatria : Jurnal Penerapan Sistem Informasi (Komputer Dan Manajemen)*, *4*(1), 224–233. https://doi.org/10.30645/KESATRIA.V4I1.134

DM, MOHD. Y., Addermi, A., & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling (JPDK)*, *4*(5), 8018–8023. https://doi.org/10.31004/JPDK.V4I5.7977

Dwiyatno, S., Sari, A. P., Irawan, A., & Safig, S. (2019). PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI. *Jurnal Sistem Informasi Dan Informatika (Simika)*, *2*(2), 64–80. https://doi.org/10.47080/SIMIKA.V2I2.606

Gunawan, R. Z., & Najicha, F. U. (2022). PERAN PENDIDIKAN KEWARGANEGARAAN DALAM MEMBANGUN KARAKTER MORAL PELAJAR DI ERA MODERN. *Jurnal Kewarganegaraan*, *6*(1).

Gusti, I., Suanti, A., Singgi, K., Suryawan, G. B., Nyoman, I., & Sugiartha, G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339. https://doi.org/10.22225/JKH.2.1.2553.334-339

Hanafi, F. (2021). *SERANGAN SIBER DI MASA PANDEMI: BANYAK AGRESI MINIM PROTEKSI | Al-Mishbah: Jurnal Ilmu Dakwah dan Komunikasi*. Al-Mishbah: Jurnal Ilmu Dakwah Dan Komunikasi. https://doi.org/https://doi.org/10.24239/al-mishbah.Vol17.Iss1.217

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143–158. https://doi.org/10.33164/IPTEKKOM.22.2.2020.143-158

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42–52. http://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/58

Kirani, A. P., & Najicha, F. U. (2022). Pentingnya Pendidikan Kewarganegaraan sebagai Pedoman dalam Menghadapi Era Society 5.0 Mendatang. *Jurnal Educatio FKIP UNMA*, *8*(2), 767–773. https://doi.org/10.31949/EDUCATIO.V8I2.2391

Pratama, M. I., & Najicha, F. U. (2022). MENINGKATKAN KESADARAN BELA NEGARA PADA SETIAP INDIVIDU DENGAN NILAI-NILAI PANCASILA PADA ERA GLOBALISASI SAAT INI. *Jurnal Kewarganegaraan*, *6*.

Rahmawati, I. (2017). ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) DALAM PENINGKATAN CYBER DEFENSE. *Jurnal Pertahanan & Bela Negara*, *7*(2), 35–50. https://doi.org/10.33172/JPBH.V7I2.1

79
Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/POLITEIA.V14I1.6351
Yasinta, Q., & Najicha, F. U. (2022). Inkonsistensi Pendidikan Kewarganegaraan Indonesia di Era Society 5.0. *Jurnal Kewarganegaraan*, *6*. http://download.garuda.kemdikbud.go.id/article.php?article=3034507&val=20674&title=Inkonsistensi%20Pendidikan%20Kewarganegaraan%20Indonesia%20di%20Era%20Society%2050
Zulfa, A., & Najicha, F. U. (2022). Urgensi Penguatan Identitas Nasional dalam Menghadapi Society 5.0 di Era Globalisasi. *Jurnal Kalacakra: Ilmu Sosial Dan Pendidikan*, *3*(2), 65–71. https://doi.org/10.31002/KALACAKRA.V3I2.6267