Nusantara Journal of Multidisciplinary Science
Vol. 1, No. 5, Desember 2023
Hal 1344-1351
E-ISSN: 3024-8752
P-ISSN: 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Pentingnya *Cybersecurity* di Era Society 5.0

Jeremiah Marvin Kapoyos[1], Dimas Abimanyu Prasetyo[2], Mochamad Reyhan Gusnaldi[3], Fried Sinlae[4]
[1,2,3,4] Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Article Info

Article history:

Received Desember 15, 2023
Revised Desember 20, 2023
Accepted Desember 23, 2023

Kata Kunci:

Cyber security,
Cyber Crime,
Era Society 5.0

Keywords:
Cyber security,
Cyber Crime,
Era Society 5.0

ABSTRAK

Ancaman dunia maya mencakup bahaya yang mengancam kerahasiaan dan integritas seseorang dan perusahaan. Saat ini, kejahatan tidak hanya terjadi secara langsung, seperti pencurian, atau lainnya mereka sekarang dapat berkembang dalam dunia digital dan dilakukan oleh spesialis komputer dan teknologi informasi. Salah satu tujuan keamanan cyber adalah untuk melindungi jaringan, perangkat, dan program dari berbagai serangan cyber serta dari pengumpulan data pengguna yang tidak sah. Metode yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif. Pada Jurnal ini membahas tentang penting nya cyber security dalam era Society 5.0. Era Society 5.0 ini menyediakan masyarakat untuk mengetahui betapa penting nya Cyber Security pada era society 5.0 ini, dengan memberikan beberapa upaya untuk melindungi informasi pribadi. Masa-masa dimana masyarakat Era revolusi industri 4.0 memunculkan 5.0 yang merupakan kemajuan dari masa tersebut. Jaringan cerdas diterapkan di seluruh rantai produksi dan proses dikontrol secara mandiri melalui integrasi mesin, alur kerja, dan sistem yang menjadi landasan Industri 5.0. Memasukkan kemajuan teknis baru dan memperhatikan bagaimana teknologi berintegrasi dengan elemen lain adalah dua tujuan utama sistem masyarakat 5.0. Segala sesuatu yang berkaitan dengan penyelenggaraan bimbingan dan konseling, khususnya penciptaan layanan konseling internet, diharapkan dapat mengikuti tren perkembangan masyarakat saat ini. Seiring dengan perkembangan teknologi informasi yang pesat, keamanan cyber menjadi sangat penting. Ada kelebihan dan kekurangan menggunakannya di dunia internet. Perundang-undangan Indonesia mengatur penggunaan teknologi informasi dan komunikasi, dan masih banyak serangan cyber. Perlu ada kerja sama antara berbagai pihak pemerintah dan masyarakat yang secara langsung menggunakan teknologi informasi, dan setiap orang harus bertanggung jawab atas penggunaan teknologi informasi.

ABSTRACT

Cyber threats include dangers that threaten the confidentiality and integrity of individuals and companies. Nowadays, crimes do not only occur directly, such as theft, or others, they can now develop in the digital world and are carried out by computer and information technology specialists. One of the goals of cyber security is to protect networks, devices and programs from various cyber attacks as well as from unauthorized collection of user data. The method used in this research is a qualitative descriptive method. This journal discusses the importance of cyber security in the Society 5.0 era. The Society 5.0 era provides the public with an understanding of how important Cyber Security is in the Society 5.0 era, by providing several efforts to protect personal information. The times when society in the Industrial Revolution Era 4.0 gave rise to 5.0 which was progress from that period. Smart networks are implemented throughout the production chain and processes are controlled autonomously through the integration of machines, workflows and systems that form the basis of Industry 5.0. Incorporating new technical advances and paying attention to how technology integrates

with other elements are the two main goals of society 5.0 systems. Everything related to the provision of guidance and counseling, especially the creation of internet counseling services, is expected to follow current societal development trends. Along with the rapid development of information technology, cyber security has become very important. There are advantages and disadvantages to using it in the internet world. Indonesian legislation regulates the use of information and communications technology, and there are still many cyber attacks. There needs to be cooperation between various government and community parties who directly use information technology, and everyone must be responsible for the use of information technology.

Corresponding Author:

Fried Sinlae
Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya,
Bekasi, Indonesia
Email: fried.sinlae@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Tujuan dari Era society 5.0 adalah untuk meningkatkan kualitas hidup penduduk dan memberikan kenyamanan bagi manusia melalui penggunaan teknologi seperti contoh Internet of Things (IoT) dan Artificial Intelligence (AI). Karena hampir semua aspek kehidupan manusia menggunakan internet, termasuk ekonomi dan sosial, keamanan informasi pengguna sangat penting. Selain itu, perkembangan teknologi telah mengubah kehidupan manusia. Masyarakat sekarang beralih ke kehidupan digital, yang mana segala sesuatu dapat dilakukan di dunia maya, meskipun orang biasanya berfokus pada lingkungan lokal mereka, karena pengetahuan tentang keamanan informasi semakin meningkat di era teknologi 5.0. Ancaman dunia maya mencakup bahaya yang mengancam kerahasiaan dan integritas seseorang dan perusahaan. Saat ini, kejahatan tidak hanya terjadi secara langsung, seperti pencurian, atau lainnya; mereka sekarang dapat berkembang dalam dunia digital dan dilakukan oleh spesialis komputer dan teknologi informasi. Orang-orang yang tidak bertanggung jawab sekarang dapat menggunakan komputer, yang dulunya digunakan untuk pekerjaan dan pengumpulan data. Salah satu tujuan keamanan *cyber* adalah untuk melindungi jaringan, perangkat, dan program dari berbagai serangan *cyber* serta dari pengumpulan data pengguna yang tidak sah.[1]

Data yang dikumpulkan dari sistem monitoring trafik IDSIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) menunjukkan bahwa jumlah insiden serangan dunia digital di Indonesia mencapai 1 Juta dan meningkat setiap hari nya disebabkan lemahnya sistem yang tidak diketahui. Dari tahun 1998 hingga 2009, 2.138 orang diberikan peluang untuk bergabung dengan sistem domain pemerintahan. Serangan internet atau kejahatan internet telah menyerang berbagai platform di Indonesia, termasuk jejaring social media seperti Twitter, Instagram, Tiktok dan yang lainnya. Sebagai pengguna, Anda mungkin memiliki sejumlah besar data pribadi yang tidak boleh dibagikan secara global, dan individu yang tidak bertanggung jawab dapat menyalahgunakannya. Pengguna cerdas dapat membantu

mengurangi kejahatan online. Studi berjudul "Pentingnya *Cyber security* dalam era Society 5.0" akan memaparkan betapa penting nya ilmu keamanan digital atau *Cyber security* ini.[1]

2. METODE

Metode yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif. Pada Jurnal ini membahas tentang penting nya *cyber security* dalam era *Society* 5.0. Era *Society* 5.0 ini menyediakan masyarakat untuk mengetahui betapa penting nya *Cyber Security* pada era society 5.0 ini, dengan memberikan beberapa upaya untuk melindungi informasi pribadi.

3. HASIL DAN PEMBAHASAN

3.1 Cyber Security di Indonesia

Indonesia telah memiliki struktur dan kebijakan untuk *cyber security*, yang dijalankan oleh anggota komunitas resmi dan juga entitas pemerintah. Kementerian Komunikasi dan Informatika (Kemkominfo) bertanggung jawab untuk mengoordinasikan strategi *cyber security*. Direktorat Keamanan Informasi, Tim Penanggulangan Insiden Keamanan Infrastruktur Internet Indonesia, dan Tim Koordinasi Keamanan Informasi adalah tiga lembaga pemerintah yang terlibat dalam *cyber security* di Indonesia[2]. Pada tahun 2019, sebanyak 290,3 juta insiden *cyberattack* dilaporkan oleh Badan Siber dan Sandi Negara (BSSN). Jika dibandingkan dengan 232,4 juta kasus pada tahun sebelumnya, jumlah tersebut meningkat drastis. Demikian pula, telah terjadi peningkatan dalam laporan polisi tentang *cybercrime* ke Badan Reserse Kriminal (Bareskrim) Kepolisian Republik Indonesia (Polri). Di Patrolisiber, situs web Bareskim untuk melaporkan kejahatan siber, ada 4.586 laporan polisi yang masuk pada tahun 2019. meningkat dari 4.360 laporan yang diterima pada tahun 2018. Upaya untuk mendapatkan akses atau kontrol yang tidak sah atas sistem atau jaringan komputer dikenal sebagai *cyberattack*. Sebaliknya*, cybercrime* adalah tindakan melanggar hukum yang mengeksploitasi sistem atau jaringan komputer sebagai target untuk menimbulkan kerugian materiil maupun imateriil pada korban. *Cybercrimes* dan *cyberattacks* keduanya dianggap sebagai ancaman siber, meskipun tidak semuanya diklasifikasikan secara formal sebagai kejahatan.[3]

Mengingat tingkat *cyber security* di Indonesia, kebijakan yang mengatur berbagai aspek keamanan siber dalam peraturan yang mengatur penggunaan perangkat teknologi perekam percakapan sangat diperlukan. Hal ini mencakup lokasi dokumen yang banyak digunakan yang menjadi acuan untuk menerapkan strategi keamanan arsip, persyaratan infrastruktur yang harus dipenuhi agar sesuai dengan standar internasional ketika terjadi *cyberwarfare*, di samping pertahanan perimeter yang memadai, perangkat pemantau komunitas, sistem manajemen informasi dan kejadian yang membantu melacak berbagai kejadian jaringan yang berkaitan dengan insiden keamanan, dan penilaian keamanan komunitas yang berperan sebagai kontrol dan pengukuran keamanan[4].

3.2 Betapa Pentingnya Cyber Security di Era Society 5.0

Masa-masa dimana masyarakat Era revolusi industri 4.0 memunculkan 5.0 yang merupakan kemajuan dari masa tersebut. Jaringan cerdas diterapkan di seluruh rantai produksi dan proses dikontrol secara mandiri melalui integrasi mesin, alur kerja, dan sistem yang menjadi landasan Industri 5.0. Memasukkan kemajuan teknis baru dan memperhatikan bagaimana

teknologi berintegrasi dengan elemen lain adalah dua tujuan utama sistem masyarakat 5.0. Segala sesuatu yang berkaitan dengan penyelenggaraan bimbingan dan konseling, khususnya penciptaan layanan konseling internet, diharapkan dapat mengikuti tren perkembangan masyarakat saat ini[5].

Untuk mengamankan lingkungan *cyber*, organisasi, dan aset pengguna, *cyber security* merupakan kombinasi alat, kebijakan, konsep keamanan, upaya perlindungan keamanan, pedoman, teknik manajemen risiko, aktivitas, pelatihan, praktik terbaik, jaminan, dan teknologi. *Cyber security* terdiri dari peralatan komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan semua informasi yang dikirim dan/atau disimpan di lingkungan siber sebagai aset organisasi dan pengguna[6].

Kesadaran keamanan siber, yang didefinisikan sebagai tingkat pemahaman pengguna akan pentingnya keamanan informasi dan kewajiban mereka untuk menerapkan tingkat pengendalian informasi yang tepat untuk melindungi data dan jaringan organisasi, merupakan metodologi untuk melatih pengguna internet agar peka terhadap berbagai ancaman siber dan kerentanan komputer dan data terhadap ancaman ini. Sejumlah besar serangan terjadi setiap hari, meskipun faktanya mayoritas orang yang menggunakan komputer, tablet, dan ponsel pintar untuk mengakses Internet tampaknya percaya bahwa ini adalah tempat yang aman. Internet menjadi lebih rentan terhadap peretasan, serangan siber, dan kelemahan keamanan[7].

Cyber security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungidan meminimalkan gangguan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun *cyber attack*. *Cyber security* merupakan upaya untuk melindungi informasi dari adanya cyber attack, adapun elemen pokok *cyber security* adalah:

1. Dokumen security policy merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. Information infrastructure merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah router, switch, server, sistem operasi, database, dan website.
3. Perimeter Defense merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan firewall.
4. Network Monitoring System merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi.
5. System Information and Event Management merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. Network Security Assessment merupakan elemen *cyber security* yang berperan sebagai mekanisme kontrol dan memberikanmeasurement level keamanan informasi.
7. Human resource dan security awareness berkaitan dengan sumber daya manusia dan awareness-nya pada keamanan informasi[8].

Dalam hal tingkat keamanan siber, langkah-langkah seperti menempatkan dokumen yang digunakan secara luas yang berfungsi sebagai panduan untuk menerapkan semua strategi yang relevan harus diperhitungkan. Kebijakan-kebijakan ini harus mengatur berbagai aspek keamanan siber dalam peraturan yang mengatur penggunaan teknologi perekaman

percakapan. Selain pertahanan perimeter yang memadai, ada kontrol dan pengukuran keamanan lainnya seperti sistem manajemen informasi, penilaian keamanan komunitas, dan keamanan arsip. Persyaratan infrastruktur juga harus dipenuhi untuk memenuhi standar global dalam hal perang siber. Perlindungan siber diperlukan dalam komunitas siber untuk mengurangi dan menjaga semua statistik data karena sejumlah ancaman terhadap server laptop, termasuk pencuri data, pencurian data pribadi, peretasan situs web, dan struktur elektronik untuk pengguna internet[4].

3.3 Kebijakan dan Hukum *Cyber Security* di Indonesia

Kejahatan yang memanfaatkan kemajuan teknologi komputer, khususnya internet, dikenal sebagai cybercrime. Berdasarkan kecanggihan perkembangan teknologi internet, cybercrime didefinisikan sebagai perbuatan melawan hukum yang memanfaatkan teknologi komputer. Karena Indonesia adalah negara hukum, maka segala aktivitas negara dan masyarakat selalu diutamakan sesuai dengan hukum. Indonesia selalu berusaha untuk melakukan amandemen terhadap hukum pidana, dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) adalah salah satu upaya tersebut. Karena masyarakat sangat bergantung pada penyelenggaraan kegiatan di bidang teknologi berbasis komputer, dan karena penyelenggaraan tersebut sering kali melibatkan pelanggaran hak asasi manusia[9].

Ketidaktahuan akan kemungkinan serangan siber yang dapat melumpuhkan infrastruktur penting, termasuk sistem radar penerbangan di Bandara Internasional Soekarno-Hatta yang telah mengalami beberapa kali gangguan. Serangan semacam itu terhadap infrastruktur penting negara bukanlah hal yang baru. Menetapkan kebijakan yang mengatur berbagai aspek keamanan siber dalam kebijakan yang berbeda sangat penting dalam kaitannya dengan kebijakan keamanan siber Indonesia.

Pemerintah Indonesia telah menangani kejahatan siber terkait komputer melalui sejumlah undang-undang dan tindakan, seperti berikut ini:

1. Undang-Undang Nomor 11 Tahun 2008 Undang-Undang Nomor 15 Tahun 2002 tentang Pencucian Uang. Pencucian uang dilakukan untuk mengubah dana ilegal menjadi dana legal, semisal dana hasil korupsi, penjualan narkotika, pencurian mobil, dan perampokan.Proses pelaksanaan penyidikan pencucian uang dilakukan dengan mudah oleh aparatur negara atau polisi, namun faktanya tidak dapat mengurangi tingkat kejahatan korupsi di Indonesia.tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 15 Tahun 2002 tentang Pencucian Uang. Pencucian uang dilakukan untuk mengubah dana ilegal menjadi dana legal, semisal dana hasil korupsi, penjualan narkotika, pencurian mobil, dan perampokan. Proses pelaksanaan penyidikan pencucian uang dilakukan dengan mudah oleh aparatur negara atau polisi, namun faktanya tidak dapat mengurangi tingkat kejahatan korupsi di Indonesia.
3. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta. Pembajakan softwareadalah salah satu kasus yang paling banyak terjadi di Indonesia dengan alasan mahalnya harga software asli. Meski tindak pembajakan sudah dikategorikan sebagai tindak pidana pada pasal 72 ayat (3) dengan pidana penjara paling lama 5 tahun dan atau denda paling banyak sebanyak lima ratus juta rupiah, nyatanya pembajakan dianggap sebagai hal biasa di Indonesia.

4. Undang-Undang Nomor 28 Tahun 2014 tentang Telekomunikasi.
5. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran.

Dalam rangka membangun landasan hukum yang mampu mengatasi ancaman siber yang kompleks, dinamis, dan multidomain, perlu adanya penguatan kebijakan dalam bentuk undang-undang yang menjelaskan dan mempertegas domain siber sebagai salah satu komponen domain kedaulatan Indonesia. Mengingat kompleksitas, sifat dinamis, dan multidomain ancaman siber terhadap keamanan, pertahanan, dan kepentingan nasional Indonesia, maka undang-undang tersebut harus dapat bekerja dengan otoritas, kekuatan, dan semua pihak terkait. Pemerintah juga harus segera menyatukan semua hukum dan aturan yang berkaitan dengan kepentingan nasional, pertahanan, dan keamanan, termasuk yang berkaitan dengan infrastruktur dan barang-barang penting negara[10].

"Terwujudnya Indonesia yang berdaulat, mandiri, dan berkepribadian berlandaskan gotong royong" adalah tujuan kebijakan pertahanan untuk pertumbuhan pertahanan negara. Tujuh misi pembangunan pertahanan menjadi sarana untuk mencapai tujuan tersebut, antara lain:

a) Mengakui bahwa keamanan nasional dapat menegakkan kedaulatan wilayah, menjaga kemandirian ekonomi dengan melindungi sumber daya maritim, dan merepresentasikan identitas Indonesia sebagai negara kepulauan,
b) Membangun masyarakat yang progresif, adil, dan demokratis yang berlandaskan supremasi hukum,
c) Mengakui perlunya politik luar negeri yang bebas aktif dan memperkuat identitas bangsa bahari,
d) Mengakui standar hidup Indonesia yang tinggi,
e) membangun negara yang berdaya saing,
f) Membangun negara maritim Indonesia yang otonom, kuat, dan berbasis kepentingan nasional; dan
g) Mengakui keberadaan masyarakat yang berkepribadian dalam kebudayaan[11].

3.4 Strategi Penguatan untuk Cyber Security di Indonesia

1. Peningkatan Ilmu Pengetahuan di Indonesia
   Sebagai pengguna internet, sangat penting untuk memahami pentingnya menjaga keamanan *cyber*. Tujuan dari upaya untuk meningkatkan pengetahuan tentang keamanan *cyber* adalah untuk membantu orang menghindari pelanggaran *cyber*. Karena semua aktifitas kehidupan bergantung pada teknologi informasi, memerangi *cybercrime* merupakan keharusan bagi semua pemerintah dan individu. Ini tentunya memerlukan kerja sama dari semua pihak, baik pemerintah maupun individu, dan masyarakat secara keseluruhan. Pemerintah membentuk komunitas keamanan *cyber* untuk mencegah, melawan, dan mendeteksi potensi serangan *cyber* secepat mungkin untuk meningkatkan ketahanan dan keamanan nasional dan melindungi warganya[1].

2. Pembentukan Undang-Undang Khusus Tindak Pidana Siber
   Indonesia memerlukan undang-undang khusus untuk tindak pidana siber. Regulasi khusus ini mengatur semua tindak pidana di bidang TI dan komunikasi, termasuk tindak pidana yang berkaitan dengan kerahasiaan, integritas, dan ketersediaan data atau sistem komputer atau sistem elektronik; pedoman pemidanaan; hukum acara yang mengatur prosedur

penyelidikan dan penyidikan TI dan komunikasi, termasuk penggeledahan dan penyitaan alat bukti digital; dan kolaborasi internasional dalam bidang TI dan komunikasi. Ini disebabkan oleh fakta bahwa Indonesia memiliki celah hukum untuk menangani serangan siber dan situasinya rentan. Indonesia membutuhkan undang-undang keamanan siber yang komprehensif karena undang-undang sebelumnya membagi tanggung jawab ke beberapa kementerian dan tidak efektif dalam mencegah ancaman dan kejahatan siber.

Nanti, UU Keamanan Siber harus dengan jelas mendefinisikan dan menjabarkan peran, tanggung jawab, dan otoritas lembaga terkait dalam menangani ancaman keamanan siber. Ketika DPR dan BSSN berbicara tentang RUU ini, mereka harus terlibat dalam dialog antara pemerintah dan swasta, juga dikenal sebagai dialog antara pemerintah dan swasta (PPD). PPD telah terbukti membantu berbagi informasi dan pengalaman yang relevan, membantu membuat kebijakan yang lebih tepat sasaran dan efektif, dan mendapatkan dukungan dari semua pemangku kepentingan[12].

4. KESIMPULAN

Seiring dengan perkembangan teknologi informasi yang pesat, keamanan *cyber* menjadi sangat penting. Ada kelebihan dan kekurangan menggunakannya di dunia internet. Perundang-undangan Indonesia mengatur penggunaan teknologi informasi dan komunikasi, dan masih banyak serangan *cyber*. Perlu ada kerja sama antara berbagai pihak pemerintah dan masyarakat yang secara langsung menggunakan teknologi informasi, dan setiap orang harus bertanggung jawab atas penggunaan teknologi informasi.

REFERENSI

[1] D. Septasari, "The Cyber Security and The Challenge of Society 5.0 Era in Indonesia," *Aisyah J. Informatics Electr. Eng.*, vol. 5, no. 2, pp. 227–233, 2023, doi: 10.30604/jti.v5i2.231.
[2] M. Rizal and Y. Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *JAS (Journal ASEAN Stud.*, vol. 4, no. 1, p. 61, 2016, doi: 10.21512/jas.v4i1.967.
[3] N. Halimah, "Cybersecurity Protection in Indonesia Standard-Nutzungsbedingungen," *Econstor J.*, no. 9, 2021, [Online]. Available: http://hdl.handle.net/10419/249442
[4] F. Indah and A. Q. Sidabutar, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)," *J. Bid. Penelit. Inform.*, vol. 1, no. 1, p. 2, 2022, [Online]. Available: https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78%0Ahttps://ejournal.kreatifcemerlang.id/index.php/jbpi/article/download/78/8
[5] N. M. A. Saputra, H. T. Hidayatullah, D. Abdullah, and Muslihati, "Pelaksanaan Layanan Cyber Counseling pada Era Society 5.0: Kajian Konseptual," *Pros. Semin. Nas. Bimbing. dan Konseling Univ. Negeri Malang*, no. 5, pp. 73–79, 2020.
[6] H. Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya Di Indonesia," pp. 95–110, 1986.
[7] A. Aziz, "Pentingnya pengetahuan cyber security untuk publik dan negara (The importance of cyber security knowledge for the public and the country)," *J. Pros. SAINTEK Sains dan Teknol.*, vol. 2, no. 1, pp. 75–82, 2023.
[8] M. Hafid *et al.*, "Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara," *Pendidik. Tambusai*, vol. 7, no. 2, pp. 9548–9556, 2023.

[9] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *J. Cakrawala Ilm.*, vol. 2, no. 10, pp. 3799–3806, 2023, doi: 10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

[10] B. R. Sanjaya *et al.*, "Pengembangan Cyber Security Dalam Menghadapi Cyber Warfare Di Indonesia," *J. Adv. Res. Def. Secur. Stud.*, vol. 1, no. 1, pp. 19–34, 2022.

[11] J. W. & R. Anang Setiyawan, "Strengtening Indonesia's Policy on National Cyber Security To Deal," *South East Asia J. Contemp. Business, Econ. Law*, vol. 15, no. 5, pp. 17–26, 2018.

[12] F. Ramadhani, "Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber," *Kult. J. Ilmu Hukum, Sos. Dan Hum.*, vol. 1, no. 1, pp. 89–97, 2023.