(2024), 2 (1): 341–344 **Scientica** 3021-8209

Jurnal Ilmiah Sain dan Teknologi

PERKEMBANGAN CYBER DI ERA GLOBALISASI

Muhammad Luqmanul Hakiem[1], Natania Bunga Prameswari Andoko[2], Iqbal Abdillah[3], Fried Sinlae[4]

202110715174@mhs.ubharajaya.ac.id , 202110715122@mhs.ubharajaya.ac.id , 202110715064@mhs.ubharajaya.ac.id, fried.sinlae@dsn.ubharajaya.ac.id

[1] Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

ABSTRACT

The development of information and communication technology in the era of globalization has had a significant impact on the development of the cyber world. This article discusses the main changes in the rapidly evolving cyber ecosystem, as globalization continues to expand the digital space. Globalization has opened the door to wider and faster connectivity, but on the other hand, cyber security challenges are also increasingly complex.

The importance of a deep understanding of cyber developments in the era of globalization is the key for individuals, companies and governments to face and manage emerging risks. Therefore, this article details several strategies and frameworks that can be implemented to mitigate cyber threats, promote digital security, and build global collaboration in facing shared challenges.

Sejarah Artikel
Submitted 4 januari 2024
Accepted 10 januari 2024
Published 11 Januari 2024

Keywords*: Impact of Information and Communication Technology on the Cyber World, Globalization Era.*

ABSTRAK

Perkembangan teknologi informasi dan komunikasi di era globalisasi telah memberikan dampak yang signifikan pada perkembangan dunia cyber. Artikel ini membahas perubahan-perubahan utama dalam ekosistem cyber yang berkembang pesat, seiring dengan globalisasi yang semakin memperluas ruang digital. Globalisasi telah membuka pintu bagi konektivitas yang lebih luas dan cepat, namun di sisi lain, tantangan keamanan cyber juga semakin kompleks.

Pentingnya pemahaman mendalam terhadap perkembangan cyber di era globalisasi menjadi kunci bagi individu, perusahaan, dan pemerintah untuk menghadapi dan mengelola risiko yang muncul. Oleh karena itu, artikel ini merinci beberapa strategi dan kerangka kerja yang dapat diterapkan untuk memitigasi ancaman cyber, mempromosikan keamanan digital, dan membangun kolaborasi global dalam menghadapi tantangan bersama.

Keyworld: Dampak Teknologi Informasi dan Komunikasi pada Dunia Cyber, Era Globalisasi.

Sejarah Artikel
Submitted 4 januari 2024
Accepted 10 januari 2024
Published 11 Januari 2024

Keyworld: Dampak Teknologi Informasi dan Komunikasi pada Dunia Cyber, Era Globalisasi.

A. Pendahuluan

Menurut ISO (International Organization for Standardization), tepatnya ISO/IEC 27032:*2012 Information technology — Security techniques — Guidelines for cybersecurity*. *Cybersecurity* atau *cyberspace security* adalah upaya yang dilakukan dalam menjaga kerahasiaan (*confidentiality*),integritas (*integrity*), dan

ketersediaan (*availability*) dari informasi di *cyberspace* . Adapun *cyberspace* merujuk pada lingkungan yang kompleks yang merupakan hasil dari interaksi antara orang, perangkat lunak, dan layanan di internet, yang didukung oleh perangkat teknologi informasi dan komunikasi (TIK) dan koneksi jaringan yang tersebar di seluruh dunia.

Sedangkan menurut **CISCO**, *cybersecurity* adalah praktik melindungi sistem, jaringan, dan program dari serangan digital. *Cybersecurity* biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasional proses bisnis.

Jadi, dapat disimpulkan bahwa *cybersecurity* atau keamanan siber sebagai tindakan untuk melindungi sistem komputer dari serangan digital atau akses ilegal. Terdapat beberapa elemen dari *cybersecurity* antara lain, *application security, information security, cloud security, network security, disaster recovery/business continuity planning, operational security,* dan *end-user education*. Elemen-elemen ini sangat penting guna memastikan keamanan *cybersecurity* secara keseluruhan, karena risiko terkena ancaman digital terus meningkat dan ancamannya pun semakin beragam. Maka dari itu, penting untuk melindungi sistem bahkan dari risiko terkecil sekalipun.

Metode

Pada metode penelitian ini metode yang digunakan adalah kualitatif. Beberapa metode yang umum digunakan oleh pelaku *cyber attack* yang menjadi ancaman *cybersecurity*.

1. ***Malware (Malicious Software)***

   Malware adalah salah satu ancaman cyber paling umum, berbentuk software berbahaya yang dibuat untuk menganggu atau merusak komputer pengguna. *Malware* seringkali menyebar melalui lampiran email atau unduhan yang nampak sah, beberapa jenis *malware* yang umum dikenal

2. ***Social engineering***

   Social engineering adalah istilah yang digunakan untuk menggambarkan serangan yang didasarkan oleh interaksi manusia, dilakukan dengan memanipulasi pengguna untuk memberikan informasi sensitif seperti *password,* jawaban untuk pertanyaan keamanan, dan lainnya. Jenis ancaman ini memanfaatkan rasa ingin tahu manusia dan memancingnya untuk melakukan hal-hal yang mungkin terasa biasa saja, tetapi sebenarnya membahayakan. Sebagai contoh, aksi *social engineering* yang marak menimpa pengguna ojek online. Modus yang dijalankan adalah dengan menelpon korban dan menanyakan kode OTP (*One Time Password*), kode ini cukup penting untuk dapat mengambil alih akun korban.

3. **Injeksi SQL**

   Injeksi SQL (*Structured Query Language*) adalah jenis ancaman *cybersecurity* yang digunakan untuk mengambil kendali dan mencuri data dari pusat data. Penjahat siber memanfaatkan kerentanan dalam aplikasi berbasis data untuk memasukkan kode

berbahaya ke dalam basis data melalui pernyataan SQL. Ini memberi mereka akses ke informasi sensitif yang terdapat dalam pusat data.

B. Hasil dan Pembahasan

Konseptualisasi Pranata Cyber Notary dalam Sistem Hukum di Indonesia Dilihat dari histori perkembangan cyber notary, maka tidak akan lepas dari awal mula diprakarsainya suatu frasa berupa "electronic notary" oleh perwakilan dari Perancis pada Trade Electronics Data Interchange System Legal Workshop di Uni Eropa pada tahun 1989. Electronic notary yang dimaksud, mempunyai artian: "Various industry associations and related peak bodies could act as an electronic notary to provide an independent record of electronic transactions between parties, i.e., when company A electronically transmits trade documents to company B, and vice versa."

Frasa tersebut berkembang maknanya dengan dikemukakannya suatu frasa yaitu "cyber notary" di Amerika Serikat oleh Information Security Committee of The American Bar Assosiation pada tahun 1994, menjelaskan: "The Committee envisaged that this proposed new legal professional would be similar to that of a notary public but in the case of the cyber notary his/her function would involve electronic documents as opposed to physical documents as opposed to physical documents. This would be an office, which be readily identifiable and recognized in every country throughout the world: i.e., as a legal professional who has been placed in a position of heightened level of trust. They would have the responsibility to undertake certain types of legal transactions than that of the public officer generally referred to in United State as a Notary.
Kedua definisi tersebut, makna baik electronic notary maupun cyber notary memiliki persamaan, yakni memiliki pemaknaan bahwa media yang digunakan dalam suatu perbuatan hukum dilakukan dengan media tak berwujud yang sifatnya elektronik sebagai pengganti dari dokumen konvensional yang berwujud kertas yang selama ini dipergunakan. Namun, gagasan cyber notary, memiliki ruang lingkup yang lebih spesifik kepada profesi hukum yang serupa oleh Notaris publik pada umumnya, dengan cakupan pekerjaan yang sama hanya saja memakai media yang berbeda, yakni dokumen elektronik.
Law Wrence Leff, menerangkan cyber notary sebagai "seseorang yang dengan mempunyai kemampuan bidang spesialis dalam hal bidang hukum dan computer dimana cyber notary tersebut merupakan sebuah konsep yang dapat memanfaatkan kemajuan teknologi yang ada dalam hal menjalankan tugas dan kewenangan Notaris".11 Transaksi yang akan dilaksanakan tidak lagi dengan suatu pertemuan tatap muka oleh para pihak, namun dengan dilaksanakannya secara elektronik melalui pranata cyber notary, penggunaan telecommunication platform dalam terciptanya transaksi dikatakan akan menimbulkan suatu efisiensi dan efektifitas tanpa mengenal hambatan ruang dan waktu untuk pihak-pihak yang melangsungkan transaksinya sewajarnya dengan transaksi yang terjadi dengan cara biasa atau konvensional.

C. Kesimpulan

UUJN-P telah menghadirkan konsep pranata cyber notary dalam hal wewenangan Notaris guna mensertifikasi transaksi yang dilakukan secara elektronik, namun dalam hal penerapan konsep pranata cyber notary ini, masih ditemukan baik adanya kekaburan pada norma yang berlaku, dan juga benturan pada norma yang berlaku. Perkembangan teknologi di bidang informasi elektronik maupun digital yang sekarang dikenal dengan era globalisasi 4.0, kewenangan Notaris yang diberikan pada UUJN-P tersebut dirasa belum cukup mendapatkan peluang, demi ikut turut serta mengembangkan efektifitas dan efisiensi dari era globalisasi digital saat ini. Konseptualisasi pranata cyber notary yang adalah salah satu metode bagi Notaris dalam menjalankan tugas dan fungsinya, untuk turut menjadi bagian dalam perkembangan teknologi di era globalisasi digital menjadi limitatif oleh peraturan yang ada saat ini. Peluang untuk konsep pranata cyber notary di Indonesia bukanlah tidak mungkin, sehingga dirasa perlu adanya urgensi pembaharuan dalam peraturan perundang-undangannya, khususnya dalam UUJN-P yang terkait pada proses pembuatan akta berbasis elektronik, maka tidak menimbulkan kekaburan dan dapat memberikan kepastian hukum dalam hal praktik konsep pranata cyber notary oleh Notaris sebagai pejabat umum Negara.

DAFTAR PUSTAKA

[1][2][3][4][5][6]

[1] K. Globalisasi, “Kajian hukum terkait penanganan cyber crime di indonesia di era konflik globalisasi,” no. November, 2023.

[2] N. I. Pertiwi, M. Batubara, and D. Harding, “Pendekatan Proses Internal dalam Menganalisa Efektivitas Organisasi pada Perusahaan Outsourcing Security,” *Psikostudia J. Psikol.*, vol. 11, no. 3, p. 488, 2022, doi: 10.30872/psikostudia.v11i3.8720.

[3] E. Budi, D. Wira, and A. Infantono, “Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0,” *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[4] S. -, “Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy,” *Yust. J. Huk.*, vol. 5, no. 1, 2016, doi: 10.20961/yustisia.v5i1.8718.

[5] R. Butarbutar, “Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya,” *J. Technol. Econ. Law*, vol. 2, no. 2, pp. 297–316, 2023.

[6] Y. Samudra, A. Hidayat, and M. F. Wahyu, “Pengenalan Cyber Security Sebagai Fundamental KeamananData Pada Era Digital,” *J. Pengabdi. Masy.*, vol. 1, no. 12, pp. 1594–1601, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/amma/article/view/1779