annujum

Annujum: Journal of Humaniora and Law
https://annujum.kjii.org

E-ISSN: 3089-2775
Vol. 1 No. 3 (2025)

Research Article

The Impact of Information Technology on Cyber Resilience

Ummu Ammelia
Universitas Sebelas Maret
E-mail: ummuammelia@uns.ac.id

Vanessa Puspitasari
Universitas Sebelas Maret
E-mail: vanessapuspitasari@uns.ac.id

Suparmi
Universitas Sebelas Maret
E-mail: suparmip@staff.uns.ac.id

Copyright © 2025 by Authors, Published by Annujum: Journal of Humaniora and Law.

Received : May 21, 2025
Revised : June 8, 2025
Accepted : June 27, 2025
Available online : July 25, 2025

How to Cite: Ummu Ammelia, Vanessa Puspitasari, & Suparmi. (2025). The Impact of Information Technology on Cyber Resilience. Annujum: Journal of Humaniora and Law, 1(3), 93–101. https://doi.org/10.63738/annujum.v1i3.12

Abstract

Developments in information technology have a significant impact on a country cyber resilience. Information technology not only increases the effectiveness of communication and information access, but also strengthens the ability to detect and respond to digital threats through the use of artificial intelligence, big data, and multi-layered security systems. However, technological advances also pose risks such as the spread of hoaxes, data theft, and the increasing frequency of cyberattacks, which can threaten political, economic, and social stability. This study uses a descriptive qualitative approach through a literature review of various relevant sources to analyze the impact of information technology on Indonesia's cyber resilience. The result indicate that increasing digital literacy, updating cybercrime regulations, and strengthening security infrastructure are important factors in creating optimal cyber resilience. Collaborative efforts between the government, the public, and the private sector are needed to leverage information technology as a strategic opportunity, rather than a threat, to national security and resilience.

Keywords: Cyber Resilience, Digital Literacy, Information Security, Cyber Regulation.

Dampak Teknologi Informasi Bagi Ketahanan Cyber

Abstrak

Perkembangan teknologi informasi memberikan dampak yang signifikan terhadap ketahanan siber suatu negara. Teknologi informasi tidak hanya meningkatkan efektivitas komunikasi dan akses

informasi, tetapi juga memperkuat kemampuan deteksi serta respons terhadap ancaman digital melalui penggunaan big data, penggunaan kecerdasan buatan, dan system keamanan berlapis. Namun, di sisi lain, kemajuan teknologi turut memunculkan risiko seperti penyebaran hoaks, pencurian data, serta meningkatnya frekuensi serangan siber yang dapat mengancam stabilitas politik, ekonomi, dan sosial. Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui studi literatur dari macam-macam sumber yang relevan untuk menganalisis dampak teknologi informasi terhadap ketahanan siber Indonesia. Hasil penelitian menunjukkan bahwa peningkatan literasi digital, pembaruan regulasi kejahatan siber, serta penguatan infrastruktur keamanan menjadi faktor penting dalam menciptakan ketahanan siber yang optimal. Upaya kolaboratif antara pemerintah, masyarakat, dan sektor swasta diperlukan agar teknologi informasi dapat dimanfaatkan sebagai peluang strategis, bukan menjadi ancaman, bagi keamanan dan ketahanan nasional.

Kata Kunci: Ketahanan Siber, Literasi Digital, Keamanan Informasi, Regulasi Siber.

PENDAHULUAN

Dalam mempertahankan dan mencapai tujuan suatu bangsa, maka dibutuhkan ketahanan siber (Aji, 2022). Ketahanan siber merupakan unsur penting yang menentukkan kemampuan sebuah bangsa dalam menghadapi dinamika lingkungan strategis yang semakin kompleks. Konsep ini mencakup kapasitas suatu negara untuk mencegah dan menangani berbagai bentuk tantangan, ancaman, hambatan, serta gangguan yang berpotensi mengganggu kelangsungan hidup bangsa. Tantangan tersebut dapat muncul dari faktor internal maupun eksternal. Dengan memiliki ketahanan siber sebuah negara dapat menjaga stabilitasnya, melindungi kepentingan negara, melindungi dari pengaruh ancaman cyber security tentunya, serta memastikan kelanjutan pembangunan dan kesejahteraan masyarakat (Sirait & Manalu, 2024).

Teknologi informasi sangat berkembang dan memawa perubahan dalam berbagai aspek kehidupan, termasuk keamanan dan pertahanan nasional. Teknologi siber membawa kemajuan teknologi yang bermanfaat di berbagai hal di dalamnya, seperti mudahnya dalam penyebaran informasi yang cepat, mudahnya komunikasi tanpa batas, peningkatan efisiensi dan produktivitas melalui kolaborasi jarak jauh, serta akses yang mudah ke berbagai informasi dan layanan (Alfi et al., 2023). Pemanfaatan teknologi informasi juga dapat meningkatkan ketahanan nasional dikarenakan memberikan dampak positif. Penggunaan teknologi informasi dalam lingkungan pemerintahan ini memunculkan istilah *electronic goverment*, hal ini terbukti bahwa toknologi informasi mampu meningkatkan pelayanan publik, transpirasi dan masih banyak lagi, oleh karena itu hal ini dapat memberikan nilai positif bagi negara. Sehingga pada akhirnya dampak positif tersebut akan membuat masnyarakat sejahtera dan tentunya akan meningkatkan ketahanan nasional (Marbandi, 2023).

Selain memberikan dampak positif, pemanfaatan teknologi informasi ini juga bersifat destruktif yang akan berdampak negatif. Adanya keterbukaan informasi di bidang politik dan ideologi akan memudahkan masuknya pengaruh negatif yang mana hal ini memudahkan masuknya pengaruh ideologi asing seperti paham liberal dan komunis yang akan mengancam ideologi pancasila. Adanya teknologi dan informasi juga memengaruhi di bidang ekonomi, meningkatkan serangan cyber security seperti penipuan online, pembobolan rekening dan lain-lain sehingga hal ini

akan berdampak negatif dan dapat menurunkan ketahanan nasional (Marbandi, 2023).

Cyber security merupakan kebijakan atau mekanisme yang memiliki tujuan untuk melindungi dan mengamankan sumber daya digital, melalui penggunaan pedoman, pendekatan manajemen risiko, tindakan, pelatihan, pelatihan, praktik terbaik, jaminan dan teknologi yang digunakan untuk melindungi sistem dan aset pengguna dari ancaman siber. Cyber security meliputi perlindungan terhadap infrastruktur, aplikasi, layanan, sistem komunikasi dan terkait informasi data yang tersimpan di ruang maya. Ardiyanti, (2021) Dalam praktiknya cyber security sebagai upaya perlindungan terhadap perangkat komputer, mobile server dan sistem elektronik atau jaringan dari berbagai ancaman serangan digital. Cyber securitiy menjadi sangat relevan sejalan dengan lonjakan penggunaan teknologi informasi dan komunikasi seperti laptop, perangkat Internet Of Things (IoT), smartphone, desktop, server, serta jaringan internet dalam kehidupan sehari-hari (Budi et al., 2021). Namun hal ini seringkali menimbulkan sebuah ancaman seperti kebocoran data hingga kelumpuhan infrastruktur negara, oleh karena itu cyber security sangat berpengaruh terhadap ketahanan suatu negara.

Penelitian ini bertujuan untuk menganalisis bagaimana teknologi informasi mempengaruhi ketahanan cyber security, baik dari sisi positif sebagai peluang maupun sisi negatif sebagai ancaman.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif dengan sifat deskriptif. Pemilihan ini merujuk pada definisi Bogdan dan Taylor (1992) sebagaimana dikutip dalam (Sujarweni, 2020:6), penelitian kualitatif adalah prosedur penelitian yang menghasilkan data deskriptif, yaitu penelitian yang bersumber dari ucapan atau tulisan dan perilaku yang dapat diamati dari subjek yang diteliti.

Tujuan pendekatan kualitatif yaitu mendapatkan pemahaman yang mendalam terkait dengan fenomena sosial budaya yang kompleks dengan fokus pada pengalaman subjektif, deskriptif numerik, dan makna daripada numerik. Untuk meneliti kajian tentang dampak teknologi informasi bagi ketahanan negara melalui berbagai metode penelitian. Peneliti dapat memeroleh data dan informasi yang valid, lengkap, kompleks dan menyeluruh untuk menghasilkan hasil penelitian yang baik. Metode penelitian yang dapat digunakan seperti, metode studi literatur dengan menggunakan data dan informasi yang sudah ada di berbagai literatur terkait kajian ini seperti buku, kajian ilmiah, dan dokumen resmi. Selain itu dalam penelitian ini, tinjauan pustaka dikumpulkan melalui pencarian artikel yang selaras dengan apa yang akan ditulis oleh penulis melalui Google Scholar, dengan tinjauan pustaka, proses penelitian dimulai dengan mencari sumber seperti artikel yang relevan melalui Google Scholar. Peneliti menggunakan kata kunci "Dampak Teknologi Informasi Bagi Ketahanan Cyber Security" untuk mencari sumber yang relevan. Dari hasil yang ditemukan peneliti menyeleksi dan mengidentifikasi artikel berdasarkan keterkaitannya dengan topik yang akan dibahas.

HASIL DAN PEMBAHASAN
Hasil Penelitian

Tabel 1
Literature Review

No.	Nama Peneliti dan Tahun	Subjek	Metode yang digunakan	Hasil Penelitian
1	Dina Septasari, (2025)	Cyber Security and The Challenge of Society 5.0 Era in Indonesia	Kualitatif deskriptif	Indonesia Adalah negara dengan cyber security yang masih lemah, sehingga memerlukan kerjasama dengan semua pihak dalam memperkuat cyber security di Indonesia, seperti pembuatan undang- undang ITE yang memperkuat cyber secutrity di Indonesia.
2	Ciara Vincha, Jati Satrio (2024)	Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia	Kualitatif	Teknologi informasi dalam dinas militer memberikan manfaat besar untuk mendukung tugas pokok, namun penggunaan yang tidak bijak dapat menimbulkan dampak negatif berupa penyimpangan perilaku dan etika.
3	Abdul Haris Subardjo (2017)	Perkembangan Individu dan Pentingnya Literasi Informasi Untuk Mendukung Ketahanan Nasional	Kualitatif	Teknologi informasi dapat mempermudah akses informasi, namun literasi informasi penting agar penyebaran data tetap benar dan mendukung ketahanan nasional.
4	Bayu Nurpatria, Abdul Rivai Ras (2022)	Kebebasan Berpendapat, Informasi Hoax terhadap	Kualitatif	Hoaks yang beredar di Indonesia sering kali menimbulkan

		Ancaman Stabilitas Ketahanan Nasional		kontroversi terhadap informasi yang diterima masyarakat, bahkan menyebabkan kebingungan. Situasi ini dimanfaatkan oleh oknum tertensu guna menanamkan fitnah dan kebencian yang pada akhirnya dapat memicu perpecahan di tengah masyarakat
5	Alvin Sudiatma, Achmad Fadhilah Putra, Mayzeb Putra (2023)	Cyber Security dan Ketahanan Nasional: Tantangan dan Solusi di Era Digital	Kualitatif	Di era digital ancaman siber muncul sebagai tantangan strategis yang langsung dan Teknik, serta berpengaruh terhadap kestabilan politik, ekonomi, dan social negara. Indonesia, sebagai negara berkembang, mengalami peningkatan serangan siber yang menargetkan infrasrtuktur vital seperti data pemerintah, system perbankan, dan layanan masyarakat.
6	Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, Femmy Silaswaty (2020)	Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesautan Republik Indonesia	Kualitatif	Di Indonesia, kebijakan khusus tentang kejahatan siber dipandang sebagai kebijakan kriminalisasi yang tepat, dengan cakupan aturan yang meliputi berbagai tindak pidana di bidang teknologi informasi dan

				komunikasi.
7	Mohammad Omer Hoshmand, Suci Ratnawati (2023)	Analisis Keamanan Infrastruktur Tknologi Infoemasi dalam Menghadapi Ancaman Cyber Security	Kualitatif	Keberhasilan perlindungan infrastruktur TI menuntut pendekatan komprehensif yang menintregasikan aspek teknis, kebijakan, dan peningkatan kapasitas sumber daya manusia, dengan Langkah proaktif guna menekan risiko serangan siber.
8	Hassanain Haykal, 2017	Pembangunan Hukum Siber Guna Pemanfaatan Ekonomi Berbasis Teknologi Informasi dalam Rangka Mewujudkan Ketahanan Nasional.	Kualitatif	Pengembangan hukum siber diharapkan dapat meningkatkan taraf hidup masyarakat, memajukan kesejahteraan umum sekaligus menjaga dan menegakkan keadilan bagi seluruh warga negara. Untuk mencapainya, negara harus menyempurnakan dan menetapkan hukum tentang pemanfaatan ekonomi berbasis teknologi informasi dan komunikasi, meningkatkan pengetahuan secara komprehensif tentang teknologi untuk berwawasan futuristic, menumbuhkan budaya hukum, dan mendorong fungsi legisiasi.

Pembahasan

Perkembangan teknologi informasi memberi kontribusi signifikan terhadap ketahanan siber, terutama dalam meningkatkan kemampuan negara dalam mendeteksi dan merespons ancaman digital. Teknologi yang semakin canggih memungkinkan pemerintah dan lembaga terkait untuk memanfaatkan sistem monitoring otomatis, kecerdasan buatan, serta analisis big data guna mengidentifikasi potensi serangan sejak dini. Seperti dijelaskan oleh Hoshmand & Ratnawati, (2023), infrastruktur TI yang didukung dengan teknologi terkini mampu memperkuat pertahanan siber melalui mekanisme pemantauan berlapis dan pembaruan keamanan berkelanjutan. Hal ini menunjukkan bahwa pemanfaatan TI secara tepat dapat menjadi pilar penting dalam menjaga stabilitas dan keamanan nasional.

Kemajuan TI juga membawa tantangan yang kompleks dan berdampak pada melemahnya ketahanan siber jika tidak seimbang dengan siapnya sumber daya manusia serta regulasi yang memadai. Fenomena hoaks, penyebaran ujaran kebencian, dan disinformasi di ruang digital menjadi ancaman serius yang dapat memicu instabilitas sosial. Nurpatria & Ras, (2022) menyatakan bahwa maraknya hoaks di masyarakat sering dimanfaatkan pihak tertentu untuk menciptakan konflik dan memecah belah persatuan. Kondisi ini menegaskan bahwa literasi digital masyarakat Indonesia masih perlu diperkuat agar mampu memilah informasi dengan benar sebelum menyebarkannya.

Transformasi digital dalam berbagai sektor kehidupan, termasuk pemerintahan, ekonomi, dan pertahanan, semakin menuntut adanya regulasi yang jelas dan adaptif. Setiyawan et al., (2020) menekankan pentingnya pembentukan undang-undang khusus mengenai kejahatan siber yang dapat menjadi pedoman hukum untuk menindak berbagai bentuk pelanggaran digital. Tanpa adanya payung hukum yang kuat, negara akan kesulitan dalam menangani pelaku kejahatan siber yang memanfaatkan celah regulasi. Oleh karena itu, pembaruan kebijakan dan penguatan regulasi menjadi langkah strategis dalam menjaga ketahanan siber.

Penguatan kapasitas individu dan masyarakat juga menjadi aspek penting dalam menjaga ketahanan nasional di era digital. Vincha & Satrio, (2024) menjelaskan bahwa literasi informasi merupakan landasan utama dalam menciptakan masyarakat yang kritis dan mampu memverifikasi informasi secara mandiri. Dengan meningkatnya akses teknologi informasi, masyarakat dituntut untuk memiliki kemampuan dalam memahami, mengevaluasi, dan menggunakan informasi secara benar guna mencegah terjadinya misinformasi yang dapat merugikan stabilitas negara.

Teknologi informasi memiliki dua sisi yang saling bertolak belakang: sebagai peluang yang memperkuat ketahanan nasional dan sebagai ancaman yang dapat merusak tatanan sosial, politik, dan ekonomi jika tidak dikelola dengan baik. Sehingga diperlukan kolaborasi antara sektor swasta, akademisi, masyarakat dan tentunya pemerintah agar tercipta ekosistem digital yang aman dan produktif. Dengan pendekatan holistik ini diharapkan mampu membentuk ketahanan siber nasional yang kuat dan adaptif dalam menghadapi berbagai ancaman siber yang terus kian berkembang.

KESIMPULAN

Berdasarkan hasil analisis dari berbagai literatur, dapat disimpulkan bahwa perkembangan teknologi informasi dapat memberikan dampak yang signifikan bagi ketahanan siber suatu negara. Pemanfaatan teknologi informasi secara positif mampu memperkuat sistem pertahanan digital melalui peningkatan monitoring, deteksi ancaman, serta penguatan infrastruktur keamanan. Namun di sisi lain, kemajuan teknologi yang tidak disertai literasi digital yang memadai berpotensi menimbulkan ancaman seperti penyebaran hoaks, pencurian data, hingga serangan siber yang menyasar infrastruktur vital.

Regulasi dan kebijakan yang adaptif menjadi elemen krusial dalam menjaga stabilitas keamanan siber. Negara perlu terus memperbarui peraturan terkait kejahatan siber supaya bisa menghadapi macam-macam bentuk ancaman yang semakin dinamis dan kompleks. Selain itu, dengan meningkatkan kapasitas sumber daya manusia melalui literasi dan edukasi secara digital merupakan langkah strategis untuk memperkuat ketahanan masyarakat dalam menghadapi arus informasi yang cepat dan tidak terbatas. Ketahanan siber hanya dapat diwujudkan melalui kolaborasi berbagai pihak, baik pemerintah, sektor swasta, praktisi teknologi, akademisi, maupun masyarakat. Pendekatan holistik dan komprehensif menjadi kunci untuk memastikan bahwa teknologi informasi tidak hanya menjadi sumber ancaman, tetapi juga peluang besar bagi kemajuan dan kemananan nasional.

DAFTAR PUSTAKA

Aji, M. P. (2022). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). Jurnal Politica, 13(02), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Aji, M. P. (2025). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). Aisyah Journal of Informatics and Electrical Engineering, 5(2), 227–233.

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2), 1–11. https://doi.org/10.7454/jkskn.v6i2.10082

Ardiyanti, H. (2021). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. Jurnal Politica, 1(1), 95–110. https://doi.org/10.22212/jp.v5i1.336

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia, 3(2), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains Dan Teknologi, 5(2), 679–686. https://doi.org/https://doi.org/10.55338/saintek.v5i2.2347

Marbandi, A. (2023). Analisis Dampak Penggunaan Teknologi Informasi terhadap Ketahanan Nasional Masyarakat di Kabupaten Bangkalan Menggunakan Pemodelan Sistem Dinamik. Jurnal Ilmiah Ilmu Manajemen, 10(2), 372–384.

Nurpatria, B., & Ras, A. R. (2022). UU ITE : Kebebasan Berpendapat , Informasi Hoax terhadap Ancaman Stabilitas Ketahanan Nasional. Jurnal Pendidikan Tambusai, 6(1972), 10220–10229.

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA. Jurnal USM Law Review, 3(2), 275–295.

Sirait, L. G., & Manalu, S. (2024). Ketahanan Nasional dan Era Digital : Peran Hukum dalam Menghadapi Kejahatan Siber di Indonesia. Mimbar Keadilan, 01(03), 84–90. https://doi.org/https://doi.org/10.5139.vol1iss3pp84

Sujarweni, V. W. (2020). Metodologi Penelitian. Pustaka Baru Press,.

Vincha, C., & Satrio, J. (2024). Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia. Jurnal Ketahanan Nasional, 30(2), 222–241. https://doi.org/http://dx.doi.org/10.22146/jkn.98563