MIMBAR KEADILAN
MKJIH

Ketahanan Nasional dan Era Digital : Peran Hukum dalam Menghadapi Kejahatan Siber di Indonesia

Luisa Guvani Sirait[1], Sahata Manalu S.H., M.H[2]

[1,2]Program Studi Ilmu Hukum FH Universitas Katolik Santo Thomas Sumatera Utara

Luisaguvani2@gmail.com

Abstract

Penelitian ini menganalisis permasalahan kejahatan siber di era digital Indonesia dan peran hukum dalam menindaklanjutinya sebagai upaya menjaga ketahanan nasional. Metode literatur review mengungkapkan berbagai kasus kejahatan siber yang mengancam keamanan individu dan berpotensi menjadi alat politik dan rekayasa ekonomi. Pemerintah Indonesia merespons tantangan ini dengan membentuk Undang-Undang Nomor 19 Tahun 2016 sebagai revisi UU ITE Nomor 11 Tahun 2008. Perubahan dan penambahan pasal dalam UU ITE merupakan langkah penyempurnaan hukum untuk melindungi kepentingan umum serta bangsa dan negara dari ancaman siber. Penelitian menyimpulkan bahwa perkembangan hukum di Indonesia terus beradaptasi dengan kemajuan zaman dan kebutuhan negara, tercermin dalam evolusi UU ITE.

Keywords

Ketahanan Nasional, Cyber Crime, Hukum, Era Digital

Introduction

Globalisasi merupakan suatu proses yang sudah berkembang dan akan terus berkembang dalam kehidupan, perkembangan inilah yang menjadi awal mula terjadinya kemajuan teknologi yang mengubah setiap aspek kehidupan individu dan negara. Kemajuan teknologi pada masa sekarang ini disebut sebagai “era digital”, pada era digital semua orang dapat mengakses berbagai macam informasi dengan cepat dan mudah. Kemajuan teknologi tidak hanya menciptakan masyarakat global yang tidak dibatasi oleh perbatasan, tetapi juga membuat hal yang tampaknya mustahil menjadi mungkin. Namun Kemudahan yang diberikan oleh kemajuan teknologi tidak selalu berdampak positif, terjadi berbagai dampak negatif yang lahir karena perkembangan ini, salah satunya kejahatan siber atau “Cyber Crime”.

Cybercrime atau kejahatan siber adalah kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan informasi (Rowe, 2019). Kejahatan siber tidak hanya membahayakan keamanan individu tetapi dunia siber juga dapat digunakan sebagai alat politik melalui penyebaran kabar bohong untuk tujuan provokasi politis maupun rekayasa ekonomi.

Yang akan menjadi tantangan bagi bangsa Indonesia untuk menjaga ketahanan nasional bangsa Indonesia.

Ketahanan Nasional sangat penting diwujudkan di Indonesia, ketahanan nasional tersebut sebagai bentuk terciptanya negara yang mampu menghadapi ganguan, tantangan serta ancaman yang terjadi ataupun akan terjadi di Indonesia. Perwujudan ketahanan nasional tersebut merupakan suatu cara untuk menciptakan kesejahteraan negara serta rakyatnya. Ancaman gangguan, ancaman, maupun tantangan yang terjadi di negara Indonesia terjadi dalam berbagai bentuk, salah satunya ancaman cybercrime tersebut.

Menurut data dari Astra Security, Indonesia digempur sekita 2.600 serangan siber per harinya pada tahun 2024, hal tersebut menyebabkan Indonesia mengalami kerugian global mencapai 9,5 triliun USD. Data tersebut juga memperkirakan kerugian ini akan meningkat menjadi 10,5 triliun USD pada tahun 2025 menurut Siber Security Francers. Indonesia sendiri berada di peringkat ke-10 secara global sebagai target serangan siber, data berikut diungkapkan dari perhitungan realtime dari Kaspersky. Di Indonesia Serangan siber tersebut terjadi dalam berbagai bentuk kejahatan dunia maya, seperti pembajakan perangkat lunak, pembobolan enkripsi, penggunaan kartu kredit curian, penipuan bank, penyebaran konten pornografi, dan bentuk kejahatan dunia maya lainnya, selain penyelundupan foto-foto porno di dunia maya, kejahatan terkait komputer lainnya di Indonesia termasuk pagejacking (mousetrapping), spam (junk mail), intersepsi, cybersquatting, dan typosquatting. Sedangkan hacking, vandalisme, serangan DoS/DDoS, penyebaran virus/worm, dan pemasangan bom logika.

Karena berbagai kasus kejahatan siber yang timbul di Indonesia, pemerintah membuat undang-undang sabagai salah satu landasan hukum yang menjadi upaya penjeratan tindakan kejahatan siber. Pemerintah Indonesia memasukkan UU Cybercrime (UU Siber) ke dalam Undang-Undang Nomor 19 Tahun 2016 dan Kode Hukum Pidana sebagai revisi dari UU ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Meskipun penanggulangan tindak cybercrime masih menghadapi kendala-kendala yang signifikan, namun landasan hukum ini dijadikan sebagai alat untuk menindaklanjuti kejahatan yang terjadi.

Sebagaimana telah diuraikan di atas bahwa Cyber Law sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana yang akan mengancam ketahanan nasional Indonesia. Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme dan lain sebagainya

Maka, dari Uraian di atas penilitian ini membahas mengenai hukum yang ada di Indonesia dalam melihat berbagai kejahatan yang terjadi di Indonesia dan pemerintahan melaksanakan hukum tersebut serta bagaimana perkembangan dan kemajuan hukum di Indonesia dalam melihat dan menangani tindak kejahatan siber tersebut, selain itu penelitian ini menjadi tantangan bagi hukum yang sudah dibentuk, dan bagaimana penyelesaian tentangan tersebut.

Sudah dilakukan berbagai penelitian terdahulu berkaitan dengan masalah yang penulis teliti, salah satu nya penelitian yang dilakukan oleh Rian Dwi Hapsari dan Kuncoro Galih Pambayun, dengan jurnal yang bejudul “Acaman Cybercrime Di Indonesia” Penelitian ini dilakukan dengan tujuan untuk medeskripsikan sejauh mana ancaman cybercrime yang terjadi di Indonesia. Dalam penelitian tersebut peneliti menemukan data bahwa terjadi perkembangan kejahatan siber dengan kerugian yang besar di Indonesia.

Selain itu penulis juga menganalisis penelitian terdahulu yang dilakukan oleh Riko Nugraha (2021) dengan jurnal yang berjudul “Perspektif Hukum Indonesia (cyberlaw) Penanganan Kasus Cyber Di Indonesia” Dalam penelitian ini penulis mendapatkan data mengenai kebijakan hukum tentang kejahatan siber (cyberlaw) yang ada di Indonesia.

Berbeda dengan kedua penelitian tersebut, penelitian yang penulis lakukan lebih berfokus kepada bagaimana penerapan secara nyata hukum tersebut di Indonesia serta

pembahasan mnegenai perkembangan dari hukum yang menyangku dengan tindak kejahtan siber, dan bagaimana tantangan yang dihadapi pemerintahan dalam menerapkan hukum tersebut kepada kejahatan yang terjadi di Indonesia.

Methodology

Penelitian ini menggunakan metode literatur review. Pada metode literatur review ini penulis menelaah dan menganalisis literatur atau karya tulis yang berkaitan dengan topik atau masalah yang akan diteliti. Metode ini digunakan untuk memperoleh pemahaman yang mendalam tentang topik tertentu, menganalisis kesimpulan yang diambil dari penelitian terdahulu, dan menyusun kerangka teoretis yang kuat untuk penelitian yang akan dilakukan (Fink, 2019). Setelah peneliti menentukan topik penelitian, selanjutnya mencari literatur yang berkaitan dengan topik penelitian dari berbagai sumber seperti jurnal, artikel, dan dokumen online.

Penulis selanjutnya membaca dan menelaah literatur yang sudah terkumpul, mencatat informasi penting, serta mengorganisasi data secara sistematis. Lalu menganalisis data dari literatur yang sudah terkumpul dan membuat sintesis atau rangkuman dari temuan-temuan yang ditemukan. Pada tahap terakhir, penulis menulis laporan hasil penelitian dengan memasukkan kesimpulan dari analisis yang telah dilakukan.

Discussion

Di era digitalisasi, dimana perkembangan komunikasi dan informasi dalam kehidupan sehari-hari yang sudah semakin mudah, cepat, dan efisien, maka hukum yang ada di Indonesia juga berkembang mengikuti era digitilasasi tersebut. Hal ini disebakan karena perkembangan tersebut memiliki dampak negative bagi berbagai aspek salah satunya aspek ketahanan nasional yang berdampak langsung bagi negara Indonesia.

Kejahatan siber atau yang sering dikenal sebagai cybercrime dalam bahasa inggris, hal tersebut merupakan dampak dari sisi negative yang dapat dirasakan oleh bangsa Indonesia. Dalam UU No 3 Tahun 2002 tentang Pertahanan Negara, telah ditetapkan bahwa ancaman dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk diantaranya ancaman siber. Cyber Crime terdiri dari berbagai jenis kejahatan, yang dimana kejahatan- kejahatan tersebut dilakukan melalui dunia maya yaitu ruang virtual yang terdapat dalam jaringan yang sering disebuat Internet. Sebagai jenis kejahatan baru yang dimungkinkan oleh teknologi informasi dan komunikasi, kejahatan dunia maya tidak mengenal batas dan dapat dilakukan di mana pun ada akses ke komputer dan koneksi internet

Jonathan Rosenoer (1997) membagi ruang lingkup Cyber Law dalam beberapa hal diantaranya: Copy right (hak cipta), Trademark (hakmerek), Defamation (penc emaran nama baik), Hate Speech (penistaan, penghinaan, fitnah), Hacking, Viruses, Illegal Access, (penyerangan terhadap computer / Optik lain), The Regulation Internet of Resource (pengaturan / Regeling sumber daya internet), Privacy (kenyamanan pribadi), Duty Care (kehati - hatian), Criminal Liability (kejahatan / Criminal dengan menggunakan Informasika dan Teknologi), Procedural Issues (yuridiksi, pembuktian, penyelidikan, dll.), Electronic Contract (transaksi elektronik), Pornography, Robbery (pencurian lewat internet), Consumer Protection (perlindungan konsumen), dan E-Commerce, EGovernment (pemanfaatan internet dalam keseharian).

Di Indonesia kejahatan dunia maya yang sering terjadi adalah penyebaran konten provokatif dan penipuan online. Pada tahun 2022, terdapat 8.831 kasus kejahatan dunia maya yang dilaporkan oleh Polri dari Januari hingga Desember (Pusiknas Polri, 2022) Kejahatan dunia maya di Indonesia meliputi pembajakan perangkat lunak, terorisme dunia maya, penipuan (termasuk penipuan berbasis dunia maya dan pelanggaran hukum transaksi elektronik), peretasan, manipulasi data, web phishing, dan serangan dunia maya terhadap sistem keamanan digital (Saragih & Siahaan, 2016). Penipuan menjadi kejahatan yang paling banyak terjadi di Indonesia. Ledakan e-commerce telah berkontribusi pada peningkatan kasus penipuan. Kejahatan dunia maya semakin memprihatinkan di Indonesia, dimana Indonesia menjadi salah satu korban terbesar serangan siber. Terdapat 1,04 juta akun membocorkan data di Indonesia pada kuartal kedua tahun 2022 saja. Jumlah kebocoran data internet di Indonesia meningkat 143% dari kuartal pertama 2022 ke kuartal kedua. Kasus kejahatan dunia maya telah memengaruhi individu dan pemerintah yang berdampak pada ketahanan nasional Indonesia.

Dengan terjadinya berbagai kejahatan siber di Indonesia maka diperlukan cara menanggulangi perbutan tersebut, hal ini diwujudkan dengan di buatnya hukum yang mengatur mengenai perbuatan kejahatan siber yang disebut sebagai Cyber Law. Cyber Law merupakan aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan kepada perorangan atau subyek hukum yang memakai teknologi internet dan memasuki dunia daring atau yang disebut sebagai dunia maya atau siber. Cyber Law tersebut berasal dari istilah hukum "Cyberspace Law". Hukum terhadap kejahatan siber tersebut sangat dinnutuhkan, dikarenakan berkaitan dengan upaya pecegahan tindak pidana yang berkaitan dengan kejahatan daring tersebut, disertai juga sebagai penanganan tindak pidana cybercrime tersebut. Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan - kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme

Berkaitan dengan cyber law, maka pemerintah membentuk hukum berupa peraturan perundang-undangan sebagai upaya untuk memeberikan efek jera terhadap pelaku kejahatan siber. Peraturan tersebut sudah diberlakukan di Indonesia sebagai bentuk bahwa hukum mengikuti perkembangan zaman yang sudah memasuki dunia online. Dimana hukum-hukum tradisional tidak mampu menjadi solusi yang efektif pada perkembangan dunia maya yang sudah sangat pesat.

Kejahatan tersebut pada dasarnya dapat dijerat berdasarkan KUHP dengan menggunakan analogi atau contoh dari beberapa pasal dalam KUHP, seperti Pasal 362 yang berkaitan dengan kasus carding, Pasal 378 yang berkaitan dengan penipuan, dan Pasal 311 yang berkaitan dengan pencemaran nama baik, dan lain-lain, dapat diterapkan dalam menangani berbagai jenis kejahatan cybercrime (Setiawan et al., 2022). Namun hukum juga memilih mengadopsi praktik untuk penanganan kejahtab siber dengan memperluas penafsiran asas dan norma hukum dalam penanganan kejahatan siber tersebut.

Dengan demikian, Pasal-Pasal dalam KUHP masih dapat digunakan tanpa perlu adanya regulasi baru untuk menangani kejahatan melalui internet. Dalam hal ini, hakim dapat menggunakan interpretasi yang luas dari pasal-pasal KUHP yang relevan dengan kejahatan cybercrime tanpa menyebutkannya secara spesifik. Selain itu, penting bagi hakim untuk mengingat prinsip-prinsip hukum yang berlaku di masyarakat dan rasa keadilan (Farah, 2021) Dalam perkembangannya, pengaturan cyber space dan kejahatan siber (ciber crimes) diatur di dalam Undang - undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi

Dan Transaksi Elektronik sebagai payung hukum. Perubahan tersebut dilakukan sebagai upaya untuk memperkuat jaminan pengakuan serta penghormatan atas hak dan kebebasan orang lain serta untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan

keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis, agar terwujud keadilan, ketertiban umum, dan kepastian hukum.

Menteri Kominfo menegaskan perubahan itu merupakan wujud tanggung jawab Pemerintah mengedepankan perlindungan kepentingan umum serta bangsa dan negara. Perubahan UU ITE memiliki arti penting sejalan dengan kebutuhan masyarakat dan perkembangan hukum baik nasional maupun global. Perubahan tersebut dilakukan karena berbagai alasan yaitu : Adanya penerapan norma-norma pidana dalam UU ITE yang berbeda-beda di berbagai tempat, UU ITE yang ada saat ini belum dapat memberikan perlindungan yang optimal bagi pengguna internet Indonesia, Pemerintah memperhatikan pembangunan ekosistem digital yang adil, akuntabel, aman, dan inovatif, Perkembangan layanan sertifikasi elektronik seperti tanda tangan elektronik, segel elektronik dan autentikasi situs web serta identitas digital, Penguatan kewenangan Penyidik Pegawai Negeri Sipil (PPNS) dalam melakukan penyidikan tindak pidana siber, khususnya yang menggunakan rekening bank dan aset digital dalam skema kejahatan.

UU ITE ini diharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.
Penegakkan hukum cybercrime sebelum disahkannya UU ITE dilakukan dengan menafsirkan cyber crime ke dalam perundangundangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi diantaranya:

a) Undang – Undang No. 14 tahun 2008 tentang Keterbukaan Informasi Publik;
b) Undang -Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
c) Undang-Undang No. 19 tahun 2002 sebagaimana telah diubah oleh Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta;
d) Undang-Undang No. 25 Tahun 2003 tentang Perubahan atas Undang – Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang sebagaimana telah diganti dengan UndangUndang No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
e) Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme;
f) Dan lain sebagainya.

Dalam praktik penegakan hukum terhadap apapun bentuk kejahatan kejahatan transnasional salah satunya kejahatan siber (cybercrimes), faktor hukum yang utama yang seringkali menjadi kendala penegakan hukum dalam praktik adalah masalah yurisdiksi. Masalah keraguan penentuan yurisdiksi dalam cyber space pun justru diakui oleh pakar hukum itu sendiri. Tien S. Saefullah yang menyatakan bahwa yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian kovensional, didasarkan pada batasbatas geografis dan waktu sementara komunikasi dan informasi multimedia bersifat internasional, multi yurisdiksi dan tanpa batas – batas geografis sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia dewasa ini sebagai salah satu pemanfaatan teknologi informasi.keterbatasan ruang lingkup regulasi menjadi kendala serius dalam penegakan hukum cybercrime undang-undang Indonesia tentang Informasi dan Transaksi Elektronik (ITE) berfungsi sebagai peraturan utama masih dianggap belum memadai untuk menjangkau semua jenis kejahatan siber yang terus berkembang.(Farhan et al., 2023)

Keterbatasan kapasitas penegak hukum juga menjadi hambatan yang signifikan. Kurangnya sumber daya manusia yang terlatih dalam bidang teknologi informasi, serta kurangnya akses terhadap teknologi yang memadai, menghambat efektivitas penegakan hukum. Tantangan sosial dan budaya juga mempersulit upaya penegakan hukum cybercrime. Minimnya literasi digital di kalangan masyarakat serta budaya permisif terhadap konten negatif di media sosial menjadi faktor-faktor yang perlu diatasi dalam upaya pemberantasan

cybercrime.(Nasution, 2024) Selain itu penanganan kasus cybercrime sering kali melibatkan berbagai instansi, namun koordinasi antar instansi belum optimal, sehingga menghambat efisiensi dalam penanganan kasus.

Dalam menghadapi permasalahan yang terjadi dalam penanganan kasus kejahatan siber tersebut, ditemukan berbagai solusi yang diusulkan. Pertama, revisi terhadap Salah satu topik utama adalah UU Informasi dan Transaksi Elektronik (ITE). Adapun perbaikan ini dapat memperluas cakupan regulasi dan mengikuti perkembangan teknologi yang terus berubah, sehingga celah hukum yang dieksploitasi oleh pelaku kejahatan siber dapat diminimalkan. Peningkatan kapasitas penegak hukum juga menjadi langkah penting. Aparat penegak hukum perlu diberikan pelatihan dan edukasi yang memadai dalam bidang teknologi informasi, sehingga mereka dapat lebih efektif dalam mengidentifikasi, menyelidiki, dan menangani kasus-kasus cybercrime dengan tepat.

Kerjasama internasional juga menjadi fokus utama dalam upaya penanggulangan cybercrime. Dengan kerjasama yang erat antar negara, pertukaran informasi dan sumber daya dapat dilakukan secara efektif, sehingga penegakan hukum dapat lebih efektif dalam melacak dan menindak para pelaku kejahatan siber yang sering kali beroperasi lintas negara. Kerjasama ini juga dapat memperkuat mekanisme penegakan hukum global untuk menangani ancaman cybercrime secara lebih holistik dan terkoordinasi.

Selain itu, penguatan koordinasi antar instansi yang terlibat dalam penanganan kasus cybercrime juga menjadi hal yang sangat diperlukan. Dengan melakukan tindakan ini, harapannya bahwa Indonesia dapat membangun ruang digital yang aman dan tidak terpengaruh oleh aktivitas kriminal online, serta meningkatkan penegakan hukum dan perlindungan korban.

Conclusion

Dalam penelitian ini telah dibahas mengenai hukum yang menjadi tonggak dasar dalam menanggulangi serta mencegah tindak kejahatan dalam dunia maya di Indonesia. Dimana penulis menemukan bahwa di Indonesia perkembangan hukum terus dilakukan mengikuti perkembangan zaman dan kebutuhan negara Indonesia. Hal tersebut diwujudkan dengan adanya perubahan Undang-Undang yang mengatur mengenai Informasi dan Teknologi Elektronik (ITE), dalam undang-undang tersebut terjadi berbagai perubahan dan penambahan pasal. Perubahan dan penambahan pasal dalam UU ITE tersebut sebagai upaya menyepurnakan hukum agar dapat mewujudkan perlindungan kepentingan umum serta bangsa dan negara oleh pemerintah.

Meskipun masih terjadi berbagai tantangan yang dihadapi dalam upaya perwujudan tersebut, sehingga pemerintah masih harus menaruh perhatian yang lebih besar dalam penanganan kejahatan siber. Tidak hanya dalam segi undang-undang, namun disertai dengan penguatan apparat penegak hukum untuk menangani kejahatan siber. Tidak hanya penguatan internal, penguatan eksternal juga perlu dilakukan dimana adanya hukum yang mengatur mengenai Tindakan siber dalam skala International. Dengan demikian, penelitian yang penulis lakukan dapat membantu dalam upaya penegakan hukum mengenai kejahatan siber, agar kejahatan yang berkaitan dengan dunia maya tidak semakin meluas dan komplek, dimana akan menyebabkan kerugian lebih besar bagi ketahanan nasional Indonesia.

References

Rowe, N. C. (2019). Honeypot deception tactics. Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings, 35–45. https://www.researchgate.net/publication/330084850_Honeypot_Deception_Tactics_Reasoning_Adaptive_Planning_and_Evaluation_of_HoneyThings

Hapsari R.D., Pambayun G.K. (2023). Ancaman Cyber Crime di Indonesia. Jurnal Konstituen, 5(1),9- 12

Nugraha R. (2021). PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA. Jurnal Ilmiah Hukum Dirgantara, 11(2)

Pamungkas A., Muliyono A., Lahangatubun N (2024). Kisis Penegakan Hukum Cybercrime di Indonesia: Hambatan dan Jalan Keluar. Delictum Jurnal : Jurnal Hukum dan Pidana Islam

Saputra D. (2024). Dinamika Hukum Dalam Penanganan Kejahatan Siber Di Indonesia. Lex Researchia, 1(1)

Gordon F, McGovern A, Thompson C and Wood MA (2022) Special issue. Beyond cybercrime: New perspectives on crime, harm and digital technologies. Guest editorial. International Journal for Crime, Justice and Social Democracy 11(1)

Naution M.A., Lasmadi S., Erwin E.,(2024). Pengaturan hukum concursus terhadap pelaku tindak pidana cyber crime. Jurnal Riset Tindakan Indonesia, 9(1)

Soerdi B.A., (2023). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Media Informasi Ditjen Potham Kemhan

Mastur. (2016). IMPLEMENTASI UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK SEBAGAI TINDAK PIDANA NON KONVENSIONAL. Jurnal Kosmik Hukum, 16(2)

Badan Nasional Pengelola Perbatasan Republik Indonesia (2024,25). Tingkatkan Keamanan Siber Nasional, BNPP Apresasi Launching CSIRT Bersama 2024 oleh Badan Siber dan Sandi Negara, https://bnpp.go.id/berita/tingkatkan-keamanan-siber-nasional-bnpp-apresasi-launching-csirt-bersama-2024-oleh-badan-siber-dan-sandi-negara

Leski Riskinaswara. (2023,15). Perubahan Kedua atas UU ITE Wujudkan Kepastian Hukum Ruang Digital. https://aptika.kominfo.go.id/2023/12/perubahan-kedua-atas-uu-ite-wujudkan-kepastian-hukum-ruang-digital/.