Journal Evidence Of Law
Vol 3 No 1 Januari-April 2024
Daya Nur Pratama
Irwan Triadi
https://jurnal.erapublikasi.id/index.php/JEL

Analisis Yuridis Terkait Peran Tni Sebagai Pertahanan Keamanan Dan Bela Negara Dalam Menghadapi Kejahatan Siber

Daya Nur Pratama, Irwan Triadi
Universitas Pembangunan Nasional Veteran Jakarta
daya.nurpratama.ipa3@gmail.com irwantriadi1@yahoo.com

ABSTRACT

This journal writing discusses the role of the TNI as a security defense and national defense in dealing with cyber crime in the digital era. This research aims to understand and analyze juridical analysis regarding the role of the TNI as a security defense and state defense in dealing with cyber crime. In writing this journal, we used a library approach research method which took as its basis the legislation in force in Indonesia and used a descriptive analysis method, namely by analyzing existing problems and the role of the Indonesian National Army as a security defense and state defense. The role of the Indonesian National Army (TNI) as a security defense and state defense in the face of cyber crime is emphasized in Law Number 34 of 2004 concerning the Indonesian National Army in chapter VI concerning the deployment and use of TNI forces. The TNI as a component of defense and security and state defense is correct in implementing existing regulations in Indonesia. However, the existence of cyber crimes that occurred in Indonesia has become an evaluation material to further improve military strategy in this case so that this conflict can be resolved quickly.
Keywords: *cyber crime, digital era, role of the TNI.*

ABSTRAK

Penulisan jurnal ini membahas tentang peran TNI sebagai pertahanan keamanan dan bela negara dalam menghadapi kejahatan siber di era digital. Penelitian ini bertujuan untuk memahami dan menganalisis terkait analisis yuridis terkait peran TNI sebagai pertahanan keamanan dan bela negara dalam menghadapi kejahatan siber. Dalam penulisan jurnal ini menggunakan metode penelitian pendekatan kepustakaan yang mengambil dasar dari perundang-undangan yang berlaku di Indonesia dan menggunakan Metode deskriptif analisis, yaitu dengan menganalisa permasalahan yang ada serta peran Tentara Nasional Indonesia sebagai pertahanan keamanan dan bela negara. Peran Tentara Nasional Indonesia (TNI) sebagai pertahanan keamanan dan bela negara dalam menghadapi kejahatan siber ditegaskan dalam UU Nomor 34 Tahun 2004 tentang tentara nasional indonesia pada bab VI tentang pengerahan dan penggunaan kekuatan TNI. TNI sebagai komponen pertahanan keamanan dan bela negara sudah tepat dalam menerapkan aturan yang ada di Indonesia. Namun adanya kejahatan siber yang terjadi di Indonesia yang menjadi bahan evaluasi untuk lebih meningkatkan strategi militer dalam kasus ini agar konflik ini dapat segera terselesaikan.
Kata Kunci: era digital, kejahatan siber, peran TNI

Pendahuluan

Perkembangan zaman di era digital terus berkembang dengan adanya teknologi yang baru dan modern. Akan tetapi, di dalam teknologi tersebut ada yang dapat mengancam pertahanan keamanan dan bela negara khususnya di Indonesia. Maka perlu adanya peranan TNI sebagai komponen pertahanan keamanan dan bela negara di Indonesia untuk dapat menghadapi kejahatan siber di era digital ini. Banyaknya kejahatan siber di Indonesia menjadikan perhatian penting bagi masyarakat untuk berhati-hati dalam menggunakan media sosial (Hasan et al., 2023). Dilansir dari Republika, adanya 46 laporan terkait kasus kejahatan siber. Kasus kejahatan siber yang dilaporkan masyarakat di antaranya penipuan jual beli barang melalui media sosial dan penipuan dengan modus "*sniffing*". Di katakana bahwa, kerugian yang dialami korban penipuan bervariasi dari ratusan ribu rupiah hingga Rp. 200.000.000 (dua ratus juta rupiah). Terkait dengan hal itu, masyarakat dihimbau untuk lebih teliti ketika ada penawaran jual beli barang melalui media sosial. Selain itu, masyarakat juga dihimbau untuk mewaspadai kasus penipuan dengan modus "*sniffing*" yang dalam beberapa waktu terakhir marak terjadi, salah satunya dengan menyebar undangan berbentuk file berekstensi APK yang dikirim melalui aplikasi perpesanan berbasis Android. *Sniffing* merupakan tindakan kejahatan penyadapan oleh peretas (*hacker*) yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mencuri data serta informasi penting seperti username dan password m-banking, informasi kartu kredit, password email, dan data penting lainnya. Modus-modus *sniffing* yang berkembang saat ini tidak hanya melalui laman internet atau website, namun sudah menggunakan aplikasi berekstensi "APK" yang disebar oleh peretas melalui perangkat telepon pintar berbasis Android.

Dalam strategi pertahanan keamanan dan bela negara berdasarkan Pasal 27 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) yang berbunyi "Setiap Warga Negara Berhak dan Wajib ikut serta dalam upaya pembelaan negara. Selanjutnya dalam Pasal 30 ayat (1) UUD NRI 1945, berbunyi "Tiap-tiap Warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara." Salah satu subyek yang berkontribusi penting dalam pertahanan dan bela negara selain warga dalam menghadapi konflik lokal ini adalah TNI, yg secara khusus sebagaimana telah diuraikan dalam Pasal 30 ayat (2) UUD NRI 1945 bahwa TNI merupakan "kekuatan utama" pada "sistem pertahanan" negara, sehingga menjadikan itu sebagai dasar konstitusional TNI yang secara khusus memiliki wewenang, tugas dan fungsi sebagai alat pertahanan negara (Umra, 2019).

Karena telah diatur secara rinci bahwa tugas pokoknya adalah berdasarkan pasal 7 ayat (1) UUD NRI 1945, yaitu menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia yang berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, serta melindungi segenap bangsa dan seluruh tumpah darah Indonesia dari ancaman dan gangguan terhadap keutuhan bangsa dan negara (Septian & Abdurahman, 2021). Dengan demikian, peran TNI dalam menghadapi kejahatan siber perlu di tingkatkan dengan bekerjasama dengan Porli atau Lembaga pendukung lainnya. Karena kejahatan siber selalu berubah-ubah dengan mengikuti perkembangan teknologi di era digital ini. Maka dari itu, penulis ingin menjelaskan terkait analisis yuridis terkait peran TNI sebagai pertahanan keamanan dan bela negara dalam menghadapi kejahatan siber di Indonesia.

Metodologi Penelitian

Penelitian merupakan suatu sarana pokok dalam pengembangan ilmu pengetahuan dan teknologi yang bertujuan untuk mengungkapkan kebenaran secara sistematis,

metodologis dan konsisten (Mulyani & Haliza, 2021). Melalui proses penelitian tersebut perlu diadakan analisa dan konstruksi terhadap data yang telah dikumpulkan dan diolah. Metode penulisan ini menggunakan pendekatan kepustakaan yang mengambil dasar dari perundang-undangan yang berlaku di Indonesia dan menggunakan Metode deskriptif analisis, yaitu dengan menganalisa permasalahan yang ada serta peran Tentara Nasional Indonesia sebagai pertahanan dan bela negara utama.

Hasil Penelitian dan Pembahasan

1. Pertahanan Keamanan dan Bela Negara

Berdasarkan Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Keamanan Negara (UU No. 3/ 2002) dijelaskan bahwa pertahanan keamanan negara adalah usaha untuk mewujudkan satu kesatuan pertahanan keamanan negara guna mencapai tujuan nasional, yaitu untuk melindungi segenap bangsa dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut serta melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. usaha pertahanan negara dilaksanakan dengan membangun, memelihara, mengembangkan, dan menggunakan kekuatan pertahanan negara berdasarkan prinsip-prinsip demokrasi, hak asasi manusia, kesejahteraan umum, lingkungan hidup, ketentuan hukum nasional, hukum internasional dan kebiasaan internasional, serta prinsip hidup berdampingan secara damai. Sebagai penjabaran konstitusi pada aspek pertahanan, bangsa Indonesia telah menyusun UU No. 3/ 2002 tentang pertahanan negara yang menetapkan bahwa sistem pertahanan negara bersifat semesta yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman (Holimin et al., 2021).

Kondisi dalam negeri dalam perkembangan ideologi, politik, ekonomi, dan sosial budaya ini dapat menimbulkan adanya ancaman dan tantangan yang berpengaruh terhadap stabilitas dan keamanan serta penyelenggaraan pertahanan negara di Indonesia. Ancaman yang perlu dicermati saat ini seperti munculnya ancaman non-tradisional seperti terorisme, penggunaan senjata pemusnah massal, spionase, masih akan mewarnai dalam penyelenggaraan pertahanan negara (Widiatmaja & Albab, 2019). Menurut penjelasan Pasal 9 ayat (1) huruf a UU No. 3/ 2002, Bela negara adalah sikap dan perilaku warga negara yang dijiwai oleh kecintaannya kepada Negara Kesatuan Republik Indonesia (NKRI) yang berdasarkan Pancasila dan UUD NRI 1945 dalam menjamin kelangsungan hidup bangsa dan negara. Bela negara adalah wujud dari pertahanan negara dan ditegaskan dalam UUD NRI 1945 pasal 27 ayat (3) dan pasal 30 ayat (1) menyatakan bahwa setiap warga negara berhak dan wajib ikut serta dalam upaya pembelaan negara. Sehingga dari amanat UUD NRI 1945 dan UU No. 3/ 2002, bela negara selain menjadi kewajiban dasar manusia, juga merupakan suatu kehormatan bagi setiap warga negara yang dilaksanakan dengan penuh kesadaran dan tanggungjawab serta sikap rela berkorban dalam pengabdian kepada negara dan bangsa.

Indonesia memiliki keunggulan dari segi geografisnya, tanah Indonesia yang cocok untuk perkebunan, pertanian, bahkan peternakan, Indonesia juga punya potensi pertambangan yang sangat baik. Kondisi alam di negara ini bisa dibilang sempurna dan

menjadi pemicu banyaknya bahan-bahan tambang bermunculan (Hidayat, 2019). Salah satu bahan tambang yang banyak terdapat di Indonesia dan cukup menarik perhatian dunia adalah emas di Papua, geothermal di Jawa Barat, batu bara di Pulau Kalimantan, minyak bumi, nikel, serta mineral tambang lainnya. Hal ini dapat mengakibatkan potensi ancaman dari luar negeri untuk Indonesia. Bangsa Indonesia terdiri dari ratusan suku daerah dan membuat negara ini memiliki banyak budaya yang sangat unik. Mulai dari bahasa lokal yang totalnya lebih dari 700 bahasa daerah, agama, pakaian, rumah adat, bahkan cara hidup masyarakat yang sangat berbeda-beda, semakin memperjelas Indonesia adalah salah satu bangsa besar. Keadaan ini sangat rentan terhadap konflik horizontal sehingga potensi ancaman dari dalam negeri pun sangat tinggi. Oleh karena itu, bangsa Indonesia memerlukan kemampuan sistem pertahanan dan keamanan negara yang kuat untuk menjamin tetap tegaknya kedaulatan NKRI.

2. Tentara Nasional Indonesia (TNI) Sebagai Pertahanan Utama Negara

Berbagai bentuk ancaman yang dilakukan oleh teroris kepada pemerintah atau pihak yang berseberangan dengan kepentingan mereka dengan melakukan berbagai cara diantaranya pembunuhan, penganiayaan, penculikan, perampokan, intimidasi dan pembajakan. Seiring dengan perkembangan situasi internasional, maka di Indonesia sendiri menggunakan pola teror oleh kelompok yang berseberangan dengan pemerintah kerap dilakukan dalam mencapai tujuan mereka menggunakan pola atau bentuk teror yang terus berkembang dengan cukup pesat. Beberapa kejadian di dalam negeri yang menimbulkan konflik horizontal dengan usaha-usaha disintegrasi oleh Organisasi Papua Merdeka (OPM) di Papua dan beberapa gerakan separatis lainnya telah menggunakan pola-pola kegiatan terorisme dalam melakukan aksi-aksinya (Dewi, 2022). Berdasarkan Pasal 7 Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU No. 34/ 2004), Tentara Nasional Indonesia (TNI) sebagai alat pertahanan negara mempunyai tugas untuk mengatasi aksi terorisme dalam gelar pola Operasi Militer Selain Perang (OMSP). Dalam upaya mengatasi aksi-aksi teror yang dilakukan oleh kelompok teroris, TNI dituntut untuk dapat bertindak cepat dan proaktif melalui berbagai upaya yang telah dilakukan agar tugas tersebut dapat terlaksana dengan baik. Efektifitas pelaksanaan tugas ini sangat tergantung pada kekuatan intelijen TNI dalam merespon setiap ancaman yang mungkin ditimbulkan oleh gerakan terorisme nasional maupun internasional.

3. Kejahatan Siber

Kejahatan siber merupakan kejahatan baru yang muncul sebagai akibat dari berkembangnya Teknologi Informasi. Kejahatan siber melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional (Butarbutar, 2023). Namun menurut penelitian lain, sarana yang dipakai tidak hanya komputer melainkan juga teknologi (Sila & Taufik, 2023). Sehingga, dengan berkembangnya teknologi di Indonesia yang sangat pesat saat ini khususnya Teknologi Informasi menjadikan kejahatan siber ini salah satu kasus yang harus benar-benar kita perhatikan dan kita waspadai. Karena bagaimanapun kejahatan seperti ini pasti akan terjadi dalam suatu wilayah atau

negara. Tergantung bagaimana usaha suatu wilayah atau negara itu dalam menanganinya.

Kasus kejahatan siber di Indonesia seiring berjalannya waktu, kasus kejahatan siber semakin marak terjadi di seluruh belahan dunia, begitupun Indonesia. Munculnya beberapa kasus "*Cyber Crime*" di Indonesia, seperti penggelapan uang di bank melalui komputer, kasus video porno yang diunggah di internet, hacker, carding atau kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet, penyebaran virus dengan sengaja di internet, *cybersquatting* yang diartikan sebagai mendaftar, menjual atau menggunakan nama domain dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain melalui internet dan kasus pencurian dokumen pemimpin negara melalui internet, semua kasus kejahatan siber ini menunjukkan gejala pergeseran masalah sosial dari dunia nyata. Tindak kejahatan ini dalam prateknya menggunakan teknologi telematika canggih yang sulit untuk dilihat dan dapat dilakukan di mana saja (Chintia et al., 2018).

Dimana modus dan motif kejahatan siber kian kompleks maka tidak ada jaminan keamanan di *cyberspace* dan tidak ada sistem keamanan komputer yang para *hacker* akan terus mencoba untuk menaklukkan sistem keamanan yang paling canggih dan merupakan kepuasan tersendiri bagi *hacker* jika dapat membobol sistem keamanan komputer orang lain (Ali, 2012). Dengan melalui situs yang dimuat oleh forbes.com, dengan judul artikelnya, yaitu "*The Top Cyber Security Risks In Asia-Pacific In* 2017" dijelaskan bahwa, varian *ransomware* terlihat menargetkan situs web yang menjalankan platform *e-Commerce Magento*. Varian ini diduga telah dikembangkan di Indonesia. Selain itu juga, disebutkan bahwa para pelaku dari Asia Pasifik sangat aktif dalam kegiatan *carding* (perdagangan kartu kredit dengan rincian rekening bank orang lain). Taktik, teknik dan prosedur (TTPs) yang terlibat dalam carding sedang dibagikan baik dalam grup tertutup di Facebook dan di forum web yang mendalam.

Bangsa Indonesia seharusnya lebih peduli dan paham, bahwa *Cybercrime* adalah kejahatan yang wajib untuk diwaspadai. Semakin sering kita menggunakan Internet, semakin besar pula kemungkinan untuk mengalami kejahatan siber ini. Oleh karena itu, diperlukan respon global yang saling terkoordinasi terhadap masalah kejahatan siber (H. Jahankhani, 2014). Indonesia perlu membentuk hukum untuk mengatur kejahatan siber. Berdasarkan sejarah kasus kejahatan siber di Indonesia, menunjukkan bahwa landasan hukum untuk *cybersecurity* masih lemah. Dibandingkan dengan negara lain, Indonesia tertinggal dalam hal kebijakan dan peraturan keamanan. UU Telekomunikasi, hanya mengenai lingkup telekomunikasi, namun tidak disebutkan infrastruktur telekomunikasi misalnya dalam konteks internet. Sehingga membuatnya sulit untuk menempatkan ke dalam konteks kasus-kasus tertentu. Meskipun lemah dalam hal legislatif, Indonesia cukup kuat dalam hal teknis dan langkah prosedural. Kerja sama internasional juga tidak dianggap sebagai masalah karena Indonesia meningkatkan kerjasama internasionalnya dengan berbagai organisasi, pakar keamanan dan forum untuk meningkatkan pemahamannya terhadap ancaman global.

Dengan meningkatnya kejahatan siber di Indonesia telah menjadikan pemerintah dan aparat hukum melakukan beberapa antisipasi untuk menekan jumlah kejahatan di internet melalui perubahan Undang-Undang sesuai perkembangan teknologi. Pemberian materi etika komputer di Perguruan Tinggi dan Pemahaman tentang kesadaran keamanan berinternet kepada para penggunanya. Namun semua kembali

kepada masing-masing pengguna teknologi informasi ini untuk sadar tentang pentingnya mengamankan data-data dan aktifitasnya (Butarbutar, 2023). Namun sayangnya tingkat kepedulian pengguna dalam menjaga keamanan teknologi informasi masih belum tinggi. Selain itu peningkatan kejahatan siber di Indonesia juga karena pengaruh kemajuan teknologi informasi itu sendiri dalam mempengaruhi budaya di Indonesia. Dengan budaya masyarakat di Indonesia yang telah mengakar kuat dan sangat mempengaruhi kehidupan sosialnya, kasus kejahatan siber ini muncul dan masuk melalui celah kelemahan pada sosial budaya masyarakat di Indonesia. Sehingga kesadaran masyarakat dalam kasus kejahatan siber ini harus bisa ditanamkan lebih kuat lagi karena harus merubah budaya masyarakatnya pula.

Kewenangan TNI ditegaskan dalam UU No. 34/ 2004 pada bab VI tentang pengerahan dan penggunaan kekuatan TNI. Telah menjadi wewenang TNI untuk melaksanakan suatu rangkaian tugas operasi yg bertujuan dalam rangka penegakan, pertahanan dan perlindungan terhadap kedaulatan nasional. TNI sebagai komponen utama dalam sistem pertahanan negara, maka sudah sewajarnya, intuisi ini diberikan kewenangan-kewenangan tertentu yang sifatnya mendukung tugas dan fungsinya dalam menjaga dan mempertahankan keutuhan bangsa dan kedaulatan wilayah negara indonesia. Secara garis besar, tugas TNI dapat dibagi menjadi dua yaitu tugas operasi militer untuk perang (OMP) dan tugas operasi militer selain perang (OMSP). Pasal 7 ayat (2) huruf b UU No. 34/ 2004 mengatur 14 bidang tugas TNI yang merupakan tugas OMSP. Sebagai contoh empat di antaranya yaitu mengatasi aksi terorisme, mengamankan obyek vital nasional strategis, memberdayakan wilayah pertahanan dan kekuatan pendukungnya secara dini sesuai dengan sistem pertahanan semesta, dan membantu tugas pemerintahan di daerah.

Dalam hal ini, pelaksanaan pada tugas pokok TNI yang dilakukan dalam OMSP telah diatur lebih lanjut pada Pasal 7 Ayat (2) huruf b UU No. 34/ 2004. Bahwasanya OMSP bertujuan untuk: (1) mengatasi gerakan Separatisme bersenjata; (2) mengatasi pemberontakan bersenjata; (3) mengatasi aksi terorisme; (4) mengamankan wilayah perbatasan; (5) mengamankan objek vital nasional yang bersifat strategis; (6) melaksanakan tugas perdamaian dunia sesuai dengan kebijakan politik luar negeri; (7) mengamankan Presiden dan Wakil Presiden beserta keluarganya; (8) memberdayakan wilayah pertahanan dan kekuatan penduduknya secara dini sesuai dengan sistem pertahanan semesta**;** (9) membantu tugas pemerintahan daerah; (10) membantu kepolisian negara republik Indonesia dalam rangka tugas keamanan dan ketertiban masyarakat yang diatur dalam undang-undang; (11) membantu mengamankan tamu negara setingkat kepala dan perwakilan pemerintah asing yang sedang berada di Indonesia; (12) membantu menanggulangi akibat bencana alam, pengungsian dan pemberian bantuan kemanusiaan; (13) membantu pencarian dan pertolongan dalam kecelakaan *(search and rescue);* (14) membantu pemerintah dalam pengamanan pelayaran dan penerbangan terhadap pembajakan, perompakan dan penyelundupan.

Namun, dalam penggunaan atau pengerahan kekuatan TNI untuk melaksanakan tugas pokok sebagaimana telah diatur dalam UU No. 34/ 2004 yang dilakukan melalui OMP maupun OMPS mengharuskan didasari oleh adanya kebijakan dan keputusan politik negara. Sebagaimana telah dicantumkan dalam Pasal 7 ayat (3) UU No. 34/ 2004. Oleh karena itu, ketentuan yang diatur pada Pasal 7 ayat (2) undang-undang tersebut terkait tugas pokok TNI dalam melakukan operasi militer, baik itu untuk perang atau selain perang dapat dilaksanakan jika terdapat suatu kebijakan dan keputusan politik

negara. Dengan begitu, ketentuan tersebut menjadi syarat mutlak untuk dilakukannya suatu operasi militer, sehingga syarat tersebut juga sebagai wujud dari negara Indonesia menganut sistem negara hukum yang demokratis.

Kesimpulan

Peran Tentara Nasional Indonesia (TNI) sebagai pertahanan dan bela negara utama dalam menghadapi kejahatan siber di Indonesia yang ditegaskan dalam UU No. 34/2004 tentang Tentara Nasional Indonesia pada bab VI tentang pengerahan dan penggunaan kekuatan TNI. Telah menjadi wewenang TNI untuk melaksanakan suatu rangkaian tugas operasi yg bertujuan dalam rangka penegakan, pertahanan dan perlindungan terhadap kedaulatan nasional. TNI sebagai komponen utama dalam sistem pertahanan negara, maka sudah sewajarnya, intuisi ini diberikan kewenangan-kewenangan tertentu yang sifatnya mendukung tugas dan fungsinya dalam menjaga dan mempertahankan keutuhan bangsa dan kedaulatan wilayah negara indonesia dari ancaman kelompok pemberontakan kejahatan siber yang dilakukan oleh para hacker. Demi untuk mencegah atau menangani terjadinya kasus kejahatan siber (yang notabene cukup membahayakan daripada kejahatan non siber), diperlukan untuk menjadi lebih pintar dan paham mengenai undang-undang atau bahaya dari suatu kejahatan tersebut daripada si pelaku. TNI sebagai komponen pertahanan keamanan negara dan bela negara sudah tepat dalam menerapkan aturan yang ada di Indonesia. Dengan tindakan-tindakan yang dilakukan, dirasa TNI sebagai garda depan sudah sangat membantu menjadi keutuhan NKRI. Maka dari itu, apa yang dilakukan TNI harus tetap dipertahankan guna mempertahankan keutuhan NKRI, bahkan hingga dapat membantu dan menuntaskan permasalahan kejahatan siber yang ada di Indonesia. Dimana dengan perkembangan di era digital ini kita sebagai masyarakat juga harus ikut membantu dengan cara selalu waspada dan berhati-hati ketika menggunakan media sosial. Sebab kejahatan siber dapat merusak sistem suatu negara.

Daftar Pustaka

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2), 299–317.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati, N. A. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology*, *2*(2), 65–69.

Dewi, I. M. (2022). Konflik dan Disintegrasi di Indonesia. *Mozaik: Kajian Ilmu Sejarah*, *6*(1).

Hasan, K., Husna, A., Muchlis, Fitri, D., & Zulfadli. (2023). Transformasi Komunikasi Massa Era Digital Antara Peluang Dan Tantangan. *Jurnal Politik Dan Pemerintahan Universitas Malikussaleh*, *8*(1), 41–55.

Hidayat, A. (2019). Sumberdaya Lahan Indonesia: Potensi, Permasalahan, dan Strategi Pemanfaatan. *Jurnal Sumberdaya Lahan*, *3*(2), 107–117.

Holimin, Dartono, & Prihantoro, D. (2021). Peran Perguruan Tinggi Dalam Meningkatkan Sistem Pertahanan Negara Melalui Pendidikan Bela Negara. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia*, *3*, 311–322.

Mulyani, F., & Haliza, N. (2021). Analisis Perkembangan Ilmu Pengetahuan dan Teknologi (Iptek) Dalam Pendidikan. *Jurnal Pendidikan Dan Konseling Universitas Pahlawan*, *3*(1), 101–109.

Septian, I. F., & Abdurahman, A. (2021). Status Hukum Penjelasan Undang-Undang Berdasarkan Sistem Peraturan Perundang-undangan Indonesia. *Jurnal Hukum Dan Pembangunan Universitas Indonesia*, *51*(3), 803–826.

Sila, G. E., & Taufik, C. M. (2023). Literasi Digital Untuk Melindungi Masyarakat Dan Kejahatan Siber. *Komversal*, *5*(1).

Umra, S. I. (2019). Penerapan Konsep Bela Negara, Nasionalisme Atau Militerisasi Warga Negara. *Lex Renaissance*, *4*(1), 164–178.

Widiatmaja, A., & Albab, U. (2019). Indonesia di Era Susilo Bambang Yudhoyono (SBY) dan Joko Widodo: Kebijakan Luar Negeri di Tengah Dinamika Lingkungan Strategis Regional. *Politica*, *10*(1), 77–93.