SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

STRATEGI KOLABORASI EFEKTIF TENTARA NASIONAL INDONESIA-KEPOLISIAN NEGARA REPUBLIK INDONESIA DALAM MENANGGULANGI ANCAMAN SIBER TIONGKOK

Ian Rizkian Milyardin[1*], Bangun P. Hutajulu[2], Hikmat Zakky Almubaroq[3]

[1]Universitas Pertahanan Republik Indonesia
[2]Universitas Pertahanan Republik Indonesia
[3]Universitas Pertahanan Republik Indonesia
* Ianrizkian@gmail.com

Korespondensi penulis: Ianrizkian@gmail.com

Abstract*. The background of this research is based on the phenomenon of domestic cyber threats that occur massively and are capable of disrupting national security stability, one of the cyber threat actors identified in Indonesia comes from a group affiliated with the Chinese state. The characteristics of threats that come from abroad, involve state actors and target multidimensional aspects, require collaborative countermeasures, the TNI-Polri as the main components of national defense and security require an effective collaborative strategy in dealing with cyber threats from China. The current problem is the lack of a pattern of cooperation, coordination and integration in dealing with cyber threats from China, as well as the capacity of national defense and cybersecurity technology and infrastructure that still needs to be improved. The purpose of this study is to analyze an effective TNI-Polri collaboration strategy to deal with cyber threats from China. The research method as an analytical approach uses a qualitative descriptive-analytical type, emphasizing the presentation of data through descriptions and then analyzed using theory as an analytical tool to find the ideal pattern of identifying gaps between applicable theories and the facts that occur. The research results and discussion indicate that the TNI-Polri collaboration in addressing cyber threats has been established and is progressing positively. However, when faced with threats from China, the collaboration remains limited to effective synergy, technological capacity and defense and cybersecurity infrastructure. Therefore, the conclusion of this research is an effective collaboration strategy through the formulation of strong and adaptive policies and regulations in cross-sector collaboration, capacity building, human resource development, and support for cutting-edge infrastructure and technology.*
Keywords*: Strategy, Collaboration and Cyber Threats.*

Abstrak. Latar belakang penelitian ini di dasari pada fenomena ancaman siber di dalam negeri yang terjadi secara masif serta mampu mengganggu stabilitas keamanan nasional, salah satu aktor ancaman siber yang teridentifikasi di Indonesia berasal dari kelompok terafiliasi dengan negara Tiongkok. Karakteristik ancaman yang datang dari luar negeri, melibatkan aktor negara dan menyasar aspek multidimensional, memerlukan upaya penanggulangan secara kolaboratif, TNI-Polri sebagai komponen utama pertahanan dan keamanan negara memerlukan suatu strategi kolaborasi efektif dalam menanggulangi ancaman siber dari Tiongkok. Permasalahan yang terjadi saat ini adalah belum terbentuknya pola kerjasama, koordinasi dan integrasi penanggulangan ancaman siber dari Tiongkok, serta kapasitas teknologi dan infrastruktur pertahanan dan keamanan siber nasional yang masih perlu ditingkatkan. Tujuan penelitian ini adalah untuk menganalisis strategi kolaborasi TNI-Polri yang efektif guna menanggulangi ancaman siber dari Tiongkok. Metode penelitian sebagai pendekatan analisis menggunakan jenis kualitatif deskriptif-analitik, menekankan penyajian data melalui deskripsi kemudian dianalisis menggunakan teori sebagai pisau analisis untuk menemukan pola ideal dari identifikasi kesenjangan antara teori yang berlaku dengan fakta yang terjadi. Hasil penelitian dan pembahasan menunjukkan bahwa kolaborasi TNI- Polri dalam menanggulangi ancaman siber sudah terbentuk dan mengarah pada perkembangan positif, namun dihadapkan pada ancaman yang datang dari Tiongkok masih terbatas pada pola sinergi yang efektif, kapasitas teknologi dan infrastruktur pertahanan dan keamanan siber. Maka kesimpulan yang diperoleh dari penelitian ini adalah strategi kolaborasi efektif diselenggarakan melalui perumusan kebijakan dan regulasi yang kuat dan adaptif dalam

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

kolaborasi lintas sektor, penguatan kapasitas, pengembangan SDM, serta dukungan infrastruktur dan teknologi mutakhir.
Kata kunci: Strategi, Kolaborasi dan Ancaman Siber.

1. LATAR BELAKANG

Perkembangan global terkait Teknologi Informatika dan Komunikasi (TIK) mempengaruhi berbagai aspek kehidupan masyarakat internasional, tatanan kehidupan sosial dalam membangun hubungan antar individu, kelompok maupun bangsa semakin dinamis. Salah satu penemuan yang mengubah tatanan sosial kehidupan masyarakat global adalah penemuan internet, di mana koneksi antar individu di berbagai wilayah di dunia dapat diselenggarakan melalui penggunaan alat digital/komputerisasi. Hal tersebut menimbulkan dampak terbentuknya suatu kampung global (*global village*) melalui dunia maya, di mana batas-batas wilayah teritorial suatu negara seolah tidak berarti pada masa kemajuan TIK saat ini. Pemanfaatan ruang-ruang dunia maya menciptakan ruang siber (*cyberspace*), tantangan terbesar pada masa ini adalah keamanan digital, melalui kejahatan di ruang siber (*cybercrime*). Kemudian berbagai jenis ancaman baru dapat dimanfaatkan pada ruang ini untuk kepentingan suatu negara melemahkan negara lainnya (*cyberwarfare*) di mana pergaulan dunia maya dijadikan satu medan peperangan baru yang lebih menguntungkan, tanpa mengorbankan prajurit, biaya peperangan murah, tanpa adanya aturan pasti yang mengikat, namun daya hancurnya sangat dahsyat di mana dapat melemahkan satu generasi bangsa dalam berbagai aspek kehidupan secara sekaligus tanpa mengorbankan jiwa manusia.

Fenomena ini terjadi di seluruh belahan dunia, ancaman siber menjadi suatu anomali dari pengembangan teknologi informasi yang awalnya diperuntukan bagi kemudahan manusia dalam menjalankan kehidupannya. Ancaman serangan siber saat ini dapat dibedakan menjadi ancaman yang terkait dengan entitas negara (*state actor*), maupun ancaman yang tidak terkait dengan entitas negara (*non-state actor*). Pada ancaman serangan siber yang terkait dengan entitas negara (*state actor*), biasanya memiliki jenis-jenis ancaman yang dilancarkan terkait dengan motivasi dengan capaian tujuan politik, militer/pertahanan negara, ekonomi maupun intelijen. Sedangkan ancaman siber yang tidak terkait dengan entitas negara (*non-state actor*) biasanya memiliki motivasi dengan capaian ekonomi, kriminal bahkan ideologi.

Salah satu entitas negara yang sering dikaitkan dengan serangan-serangan siber (*cyberattack*) di berbagai negara besar di dunia adalah negara Tiongkok. Dengan kemajuan teknologi yang dimiliki, serta strategi keamanan nasional yang mengadopsi *informationized warfare* semenjak awal tahun 2000-an, kebutuhan spionase dalam mencapai ambisi penguasaan ekonomi dan teknologi global serta kepentingan geopolitik untuk melemahkan lawan-lawannya melalui *soft power* dengan menyerang infrastruktur strategis dan perang psikologis khususnya terkait beberapa konflik yang dihadapi seperti Indo-Pasifik, Laut China Selatan, konflik Taiwan dan lain sebagainya.

Beberapa serangan siber yang dilancarkan oleh aktor-aktor yang datang dari negara Tiongkok. Beberapa diantaranya terdokumentasi dari berbagai sumber yang valid menimbulkan gangguan bagi keamanan digital nasional, salah satunya pada tahun Pada tahun 2021, kelompok Mustang Panda dilaporkan melakukan serangan siber terhadap sepuluh kementerian dan lembaga di Indonesia dengan tujuan spionase, hal ini berpotensi melemahkan kerahasiaan data strategis negara. Selanjutnya, pada tahun 2022, kelompok SharpPanda

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

menargetkan entitas pemerintah profil tinggi di Indonesia melalui penyebaran malware, sehingga menimbulkan risiko kebocoran informasi penting dan gangguan terhadap fungsi pemerintahan. Pada tahun 2023, terjadi dua insiden besar yaitu serangan Raspberry Typhoon menyasar lembaga militer (TNI) serta sistem maritim dan Granite Typhoon menyerang sistem telekomunikasi Indonesia, kedua serangan ini berimplikasi pada terganggunya keamanan data pertahanan dan stabilitas infrastruktur vital negara. Selain itu, kebocoran dokumen dari kelompok I-Soon atau Fishmonger mengungkap adanya aktivitas pengawasan dan penyusupan siber terhadap sejumlah pemerintah Asia Tenggara (termasuk Indonesia) dikategorikan sebagai spionase dan dapat mengancam stabilitas keamanan siber kawasan. Secara keseluruhan, rangkaian serangan yang terdokumentasi ini berdampak serius terhadap keamanan nasional Indonesia karena mengancam kerahasiaan negara, kedaulatan digital, serta stabilitas sektor pertahanan dan infrastruktur kritis.

Berdasarkan beberapa fenomena yang telah diuraikan, maka peneliti menemukan kondisi yang diharapkan (das sollen) bahwa ancaman siber dari negara Tiongkok dapat diantisipasi melalui kolaborasi efektif dari institusi TNI-Polri dalam bentuk gelar operasi gabungan siber yang terintegrasi dengan BSSN sehingga memiliki landasan regulasi yang kuat, serta sistem pertahanan siber semesta yang tangguh. Namun pada kenyataannya kondisi yang terjadi saat ini (das sein) adalah dalam menanggulangi ancaman siber di dalam negeri masih bersifat sektoral, di mana masing-masing institusi fokus pada tugas pokoknya masing-masing dan belum terbentuk kolaborasi yang efektif, hal ini berdampak pada kerentanan ancaman siber dari negara Tiongkok dapat berdampak sistemik dan mengganggu stabilitas keamanan dalam negeri.

Mengacu pada fakta das sollen dan das sein tersebut, maka dapat dicermati kesenjangan (gap) diantaranya belum ditemukan penelitian yang secara khusus menyoroti model kolaborasi antara TNI dan Polri dalam menghadapi ancaman siber dari negara Tiongkok, di mana sinergi kedua institusi ini merupakan kunci dalam membentuk pertahanan siber nasional yang tangguh, holistik dan adaptif. Penelitian ini menegaskan adanya celah penting yang belum terisi dalam literatur yang tersedia, yakni kebutuhan mendesak untuk merumuskan model kolaborasi TNI–Polri yang efektif sebagai respon strategis terhadap eskalasi ancaman siber dari Tiongkok terhadap Indonesia. Beberapa permasalahan yang diangkat dalam penelitian ini, diantaranya : pertama, belum kuatnya sinergi antara TNI dan Polri dalam penanggulangan ancaman siber. Kondisi saat ini di mana kesadaran pentingnya kolaborasi kekuatan dalam mengatasi ancaman siber untuk menghasilkan kekuatan yang lebih besar belum terbentuk dengan baik, salah satu bentuk kolaborasi efektif dapat diselenggarakan melalui upaya sinergi antar institusi. Sinergi menurut Steven Covey (2010) sinergi adalah kombinasi atau paduan unsur atau bagian yang dapat menghasilkan keluaran lebih baik dan lebih besar daripada dikerjakan sendiri–sendiri.

Kedua, kapasitas institusi TNI dan Polri dalam penyelenggaraan kolaborasi untuk menanggulangi ancaman siber belum ideal. Aspek kompetensi yang dibutuhkan diantaranya kemampuan teknologi, sarana dan prasarana pendukung serta sistem kelembagaan berupa kemampuan kebijakan yang saling berhubungan, maka penting untuk membangun kapasitas TNI dan Polri dalam menghasilkan kompetensi pada penanggulangan ancaman siber. Pembangunan kapasitas (capacity building) menurut Haryono, dkk (2012) kapasitas suatu lembaga dapat dilihat dari berbagai elemen yang dapat menentukan pengembangan lembaga

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

tersebut, dimensi pembangunan kapasitas, yaitu meliputi tiga dimensi diantaranya: pengembangan sumber daya manusia, penguatan organisasi serta reformasi kelembagaan.

Ketiga, belum terbentuknya strategi aplikatif dalam meningkatkan kolaborasi TNI dan Polri guna menanggulangi ancaman siber. Strategi merupakan aspek yang penting untuk mendeskripsikan tujuan yang ingin dicapai pemerintah, dalam hal ini adalah stabilitas keamanan digital nasional. Strategi menurut Lykke (1993) merupakan ekspresi koheren untuk mengidentifikasi tujuan (ends), cara (ways) dan sumber daya (means) sebagai proses penentuan rencana para pemimpin yang berfokus pada tujuan jangka panjang organisasi.

Berdasarkan ketiga persoalan tersebut di atas, maka pentingnya penelitian ini diselenggarakan agar memperoleh suatu strategi aplikatif dalam meningkatkan kolaborasi antara TNI dan Polri dalam menanggulangi ancaman siber khususnya yang datang dari negara Tiongkok, diantaranya ancaman spionase, serangan malware dan serangan terhadap infrastruktur vital. Penelitian-penelitian sebelumnya telah banyak membahas terkait pengamanan siber di Indonesia dari berbagai fenomena ancaman yang terjadi saat ini, namun pada penelitian terdahulu yang banyak dibahas secara sektoral (satu institusi tertentu), pada penelitian ini ditawarkan kebaruan (novelty) penanganan keamanan siber dilaksanakan melalui kolaborasi antara TNI dan Polri di mana menekankan pada sinergi antar institusi untuk menghadapi tantangan yang ada saat ini. Hasil penelitian ini diharapkan dapat menjadi solusi penting dalam pembangunan sistem pertahanan negara yang kuat, adaptif dan terpadu tidak dapat dilepaskan dari prinsip dasar sistem pertahanan semesta, yaitu keterlibatan seluruh komponen bangsa secara menyeluruh, berlapis dan bertingkat. Sistem pertahanan semesta tidak hanya menekankan pada salah satu unsur organisasi semata, tetapi juga menegaskan pentingnya kolaborasi kekuatan komponen bangsa secara bertingkat, dari individu/perorangan, institusi hingga integrasi antar institusi, untuk membangun daya tangkal dan ketahanan bangsa yang komprehensif.

2. TINJAUAN PUSTAKA

Teori Strategi. Menurut Arthur F. Lykke, Jr. (1993) Strategi merupakan suatu ekspresi koheren dari suatu proses yang mengidentifikasikan ends (tujuan), ways (cara) dan means (sumber daya). Ends merupakan tujuan atau hasil yang diinginkan dari strategi yang dilakukan. Istilah end-state identik dengan akhir dari tujuan strategi. Ways adalah tindakan atau metode dan proses yang dilakukan untuk mencapai tujuan. Sedangkan means adalah seluruh sumber daya yang dibutuhkan untuk melaksanakan metode dan proses tersebut. Lykke menyatakan pentingnya untuk menyeimbangkan ends, ways, dan means yang disamakannya dengan tiga fondasi dari strategi. Strategi disebut seimbang dan sedikit mengandung resiko jika dalam mencapai suatu tujuan (ends) digunakan cara (ways) yang tepat, dengan sumber daya (means) yang memadai. Mengacu pada konsep teori strategi tersebut diatas, dihadapkan pada strategi kolaborasi efektif TNI dan Polri dalam menanggulangi ancaman siber Tiongkok, strategi menjadi aspek penting dalam upaya mewujudkan konsep kolaborasi efektif yang diinginkan antara TNI dan Polri dalam menanggulangi ancaman siber dari negara Tiongkok. Upaya yang dapat dilaksanakan adalah dengan merumuskan aspek ends, ways dan means sehingga konsep

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

yang telah dibentuk dapat diaplikasikan melalui uraian aspek pembentuk konsep tersebut sebagai upaya yang koheren.

Teori Keamanan. Stabilitas keamaan digital yang terganggu dapat berpengaruh pada kedaulatan digital (digital sovereignty), mengutip pemikiran dari kajian yang dilaksanakan oleh Federico Pierucci (2025) kedaulatan digital merupakan konsep yang kompleks dan terus berkembang, yang menunjukkan bagaimana negara, korporasi, dan komunitas non-state aktor menegaskan kontrol atas dunia maya. Konsep ini beroperasi di berbagai lapisan dari fisik (kabel bawah laut, pusat data) hingga virtual (komputasi cloud, kecerdasan buatan, platform digital) menciptakan yurisdiksi digital. Berbeda dengan kedaulatan tradisional karena sifat transnasional dunia maya yang membatasi kemampuan negara untuk sepenuhnya mengontrol arus data dan infrastruktur. Namun, kemampuan menanamkan aturan dalam kode etik penggunaannya memberi peluang bagi negara untuk menegakkan nilai dan kontrolnya. Menganalisis teori keamanan nasional tersebut diatas, peneliti mengambil benang merah terkait konsep keamanan dalam menghadapi tantangan era kontemporer saat ini. Ancaman saat ini bersifat multidimensional akibat hadirnya ancaman dari multi aktor baik dari aktor negara maupun aktor non-negara yang dengan sengaja merancang gangguan keamanan agar situasi stabilitas dalam negeri terganggu, sehingga memudahkan setiap aktor untuk memperoleh kepentingannya.

Teori Perang Siber (Cyber Warfare). Karakteristik utama dalam sebuah peperangan adalah penggunaan senjata dalam upaya menyerang lawannya, namun dalam konteks perang siber, identifikasi ini penentuan apakah suatu tindakan tergolong sebagai serangan atau bukan menjadi permasalahan yang kompleks. Hal ini menjadi titik pembeda yang penting dalam memisahkan kejahatan siber (cyber crime) dengan perang siber (cyber warfare). Dalam dunia maya, definisi penyerangan dalam arti perang (war) mengacu pada penggunaan perangkat komputer yang secara khusus dirancang atau dibuat untuk menimbulkan kerusakan, luka, bahkan kematian terhadap manusia maupun objek yang menjadi sasaran penghancuran. Dengan demikian, niat, skala dampak, dan tujuan strategis menjadi indikator penting dalam membedakan antara tindakan kriminal siber biasa dan tindakan yang tergolong sebagai perang siber (Boothby, 2013). Menurut Clarke dalam Parks (2013) serangan siber kerap diartikan sebagai tindakan yang dilakukan oleh suatu negara untuk merusak sistem komputer negara lain. Namun, pandangan ini mendapat bantahan dari James Andrew Lewis, menurutnya suatu serangan siber baru dapat dikategorikan sebagai perang apabila serangan tersebut menyebabkan kerusakan fisik yang nyata serta menimbulkan kerugian atau korban jiwa.

3. METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif. Metode penelitian kualitatif dipandang paling sesuai dalam penelitian tentang strategi kolaborasi efektif TNI dan Polri dalam menanggulangi ancaman siber Tiongkok karena pendekatan kualitatif dianggap paling tepat dalam penelitian kolaborasi TNI–Polri dalam ranah siber bukan hanya soal aspek teknis pertahanan atau penegakan hukum. Fenomena ini juga menyangkut koordinasi lintas lembaga, interoperabilitas sistem, serta pembangunan kepercayaan (trust-building) antar institusi, yang sulit diukur secara numerik. Data kuantitatif atau mixed methode cenderung tidak mampu menangkap nuansa interaksi, persepsi dan dinamika sosial yang menjadi inti dari kolaborasi

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

lintas institusi tersebut. Waktu penelitian yang digunakan dalam pengumpulan dan analisis data dilaksanakan sesuai alokasi waktu yang diberikan oleh lembaga Uiversitas Pertahanan yaitu dirancang selama 5 (lima) bulan, semenjak bulan Juli sampai November tahun 2025. Daftar subjek penelitian sebagai informan dalam proses penelitian Tesis ini dipilih mewakili berbagai strata penanganan bidang siber di dalam negeri diantaranya mewakili tingkatan strategis (pengambil kebijakan) dan teknis (pelaksana lapangan) di TNI dan Polri, serta pakar akademisi, sehingga perspektif beragam tercakup.

Pengumpulan data dalam penelitian ini menggunakan pengumpulan data primer merupakan data yang diperoleh dari informasi yang dikumpulkan secara langsung pada subjek penelitian (narasumber) informasi ini diperoleh dari kegiatan wawancara langsung secara mendalam serta observasi lapangan terkait beberapa variabel yang dikumpulkan. Untuk menguji atau memeriksa keabsahan atau keterandalan data, digunakan triangulasi pemeriksaan data dengan metode triangulasi sumber dan triangulasi Teknik. Proses analisis data yang ditentukan menggunakan metode analisis data interaktif yang dikembangkan oleh Miles, Huberman dan Saldana (2014).

4. HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian.

Ancaman siber pada era kontemporer saat ini bersifat multidimensional yang menyentuh beberapa aspek secara sekaligus khususnya bidang pertahanan dan keamanan dalam negeri. Saat ini Indonesia tengah mengalami percepatan transformasi digital di berbagai sektor, peningkatan signifikan terlihat pada penggunaan media sosial, layanan publik berbasis daring, serta pemanfaatan teknologi cloud computing dan Internet of Things (IoT). Meskipun perkembangan ini memberikan banyak manfaat, di sisi lain, hal tersebut juga membuka celah baru bagi aktor siber untuk mengeksploitasi sistem, jaringan, maupun perangkat yang memiliki kerentanan keamanan. Ancaman seperti serangan phishing dan pencurian kredensial kian meningkat, dengan tujuan utama memperoleh akses tidak sah terhadap basis data yang berisi informasi sensitif, seperti identitas di KTP, data perpajakan, nomor rekening bank, hingga dokumen rahasia milik pemerintah. Informasi yang berhasil dicuri tersebut umumnya diperjualbelikan di pasar gelap digital (dark web), baik untuk kepentingan ekonomi, kejahatan, maupun agenda politik domestik.

Upaya penanggulangan ancaman siber memerlukan kapasitas institusi sebagai wujud kemampuan dalam menghadapi ancaman siber dari negara Tiongkok. TNI memiliki satuan khusus yang bertanggung jawab terhadap keamanan siber, yaitu Satuan Siber TNI, dengan kapasitas Peran satuan siber TNI diantaranya adalah :

a. Keamanan dan Pertahanan Siber. Satuan Siber TNI bertanggung jawab untuk melindungi infrastruktur dan sistem informasi TNI dari serangan siber, termasuk pencegahan, deteksi, respons, dan pemulihan dari insiden siber.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

b. Pengembangan Doktrin dan Kebijakan. Satuan ini terlibat dalam pengembangan doktrin, kebijakan, dan prosedur yang berkaitan dengan keamanan siber, agar sesuai dengan kebutuhan pertahanan nasional.

c. Pelatihan Personel. Menyelenggarakan program pelatihan dan edukasi untuk meningkatkan kompetensi personel TNI dalam bidang keamanan siber dan kemampuan teknis terkait.

Unsur Polri memiliki kapasitas dalam menangani kejahatan siber di Indonesia antara lain:

a. Direktorat Tindak Pidana Siber (Dittipidsiber) di bawah Bareskrim Polri (Badan Reserse Kriminal Kepolisian Negara Republik Indonesia) adalah lembaga yang dibentuk khusus untuk menangani kejahatan siber, meliputi penyidikan dan penindakan tindak pidana siber serta memberikan edukasi keamanan siber.

b. Badan Intelijen dan Keamanan Polri (Baintelkam Polri) yang membawahi Bidang Intelijen Teknologi yang berfokus pada deteksi dini, pemetaan ancaman, dan pengumpulan informasi strategis.

c. Divisi Teknologi Informasi dan Komunikasi (Divtik) yang membawahi Birotekinfo yang salah satu tugasnya adalah melakukan pengkajian dan pengembangan sistem serta metode dalam bidang Teknologi Informasi dan Komunikasi (TIK).

d. Kerjasama dengan Sektor Swasta dan Lembaga Internasional

Koordinasi antara TNI, Polri dan BSSN dalam menangani serangan siber sangat penting dan telah dilakukan melalui beberapa mekanisme, meskipun tantangan tetap ada. Berikut adalah beberapa aspek yang menggambarkan sejauh mana koordinasi tersebut:

a. Pembentukan tim koordinasi khusus melalui pembentukan tim penanganan insiden yang melibatkan TNI, Polri dan BSSN untuk menangani serangan siber yang berskala besar atau berdampak tinggi, yang melibatkan semua pihak dalam pengambilan keputusan dan respons cepat.

b. Pertukaran Informasi melalui sistem informasi terintegrasi, terdapat inisiatif untuk mengembangkan sistem informasi terintegrasi yang memungkinkan pertukaran informasi intelijen dan data mengenai serangan siber secara real-time antara lembaga. Pertukaran informasi mengenai ancaman, metode serangan, dan strategi mitigasi untuk memperkuat respons terhadap ancaman yang ada.

c. Peningkatan Kapasitas dan Sumber Daya Manusia, dengan bersinergi pada lembaga-lembaga pendidikan internal dengan melibatkan TNI/Polri sebagai siswa undangan untuk meningkatkan sinergi antar lembaga TNI dan Polri.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

Kondisi sinergi antara TNI dan Polri dalam penanggulangan ancaman siber saat ini sudah menunjukkan perkembangan positif, hal tersebut diidentifikasi dari telah terbentuknya unit tanggap insiden Mil-CSIRT dan CSIRT Polri. Indikasi selanjutnya adalah partisipasi aktif kedua institusi ini dalam forum keamanan siber lintas instansi dibawah koordinasi BSSN, pertukaran informasi intelijen secara real-time, serta keterlibatan dalam pengamanan siber skala besar pada perhelatan KTT G20 yang berhasil mengamankan penyelenggaraan dari ancaman siber. Namun masih terdapat beberapa kendala untuk meningkatkan sinergi antara TNI dan Polri diantaranya perbedaan budaya organisasi, berdampak pada pengambilan keputusan secara sinergis antar kedua institusi ini cukup kompleks (TNI bersifat hirarkis, Polri bersifat prosedural). Sifat ancaman siber di dunia maya sulit dibedakan dalam klasifikasi ancaman diantaranya antara UU ITE dan UU Hanneg membangun zona abu-abu dalam penanggulangan secara bersama. Selain itu, keterbatasan infrastruktur teknologi, belum mampu

Strategi kolaborasi TNI dan Polri guna menanggulangi ancaman siber, sesuai informasi-informasi yang diberikan oleh narasumber menyatakan bahwa kondisi di lapangan memerlukan pendekatan yang terstruktur dan multidimensi. Bentuk kolaborasi ideal yang diharapkan harus memiliki koordinasi struktural yang solid dengan pembentukan pusat komando gabungan *Cyber Command Center* atau *Joint Cyber Operation Center* (JCOC). Pusat komando ini memiliki fungsi sebagai simpul koordinasi yang memungkinkan terjadinya gelar operasi pengamanan siber secara terpadu dan terintegrasi. Selanjutnya, penting untuk setiap instansi memiliki perwira penghubung untuk meningkatkan intensitas komunikasi dan koordinasi serta tersedianya Protap/SOP bersama sehingga pembagian tugas dan wewenang akan terdistribusi dengan baik sesuai tugas pokok, kemampuan dan kewenangan masing-masing institusi, menghindari tumpang tindih pelaksanaan penanggulangan ancaman siber.

4.1 Pembahasan

a. Pola Kerjasama, Koordinasi dan Integrasi dalam Membentuk Sinergi TNI dan Polri pada Penanggulangan Ancaman Siber

Indikator yang dapat digunakan untuk menilai kondisi sinergi antara TNI dan Polri saat ini pada konteks penanggulangan ancaman digital dapat diketahui dari penilaian beberapa aspek pembangun sinergi diantaranya kerjasama, koordinasi dan integrasi/keterpaduan.

a. Kerjasama.

Pola kerjasama yang dapat diselenggarakan dalam kerangka kerja TNI dan Polri yang sinergis pada penanggulangan ancaman siber dari Tiongkok diantaranya melalui pembentukan kesatuan pertahanan siber terpadu yang selaras dan saling mendukung akan mengoptimalkan upaya dalam menghadapi ancaman siber yang semakin kompleks dan lintas sektoral.

1) Pola kerjasama respons cepat: Ketika serangan terdeteksi, dapat dengan cepat mengarahkan tim yang paling sesuai (misalnya, unit TNI untuk melindungi

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

sistem pertahanan, sementara unit Polri bersiap untuk investigasi). Tidak ada lagi waktu yang terbuang untuk menentukan "siapa yang bertanggung jawab".

2) Kerjasama Analisis: Setiap lembaga dapat menyumbangkan data dan intelijennya. Misalnya, data teknis dari BSSN, intelijen militer dari TNI, dan data forensik dari Polri dapat digabungkan untuk menghasilkan gambaran serangan yang paling lengkap, termasuk motif dan identitas pelaku.

3) Kerjasama pemanfaatan Sumber Daya: Sumber daya yang terbatas (anggaran, SDM ahli) dapat dialokasikan secara efisien. Dengan adanya kerjasama TNI dan Polri, duplikasi pekerjaan dapat dihindari dan setiap lembaga fokus pada keahliannya.

b. Koordinasi.

Pola koordinasi yang dapat diselenggarakan TNI dan Polri dalam menanggulangi ancaman siber dari Tiongkok diantaranya melalui pembangunan komunikasi strategis antara TNI-Polri, BSSN dan Komdigi sangat krusial dalam mendukung pertahanan siber dari Tiongkok. Komunikasi yang efektif memastikan semua pihak memiliki pemahaman yang sama, bertindak secara terkoordinasi dan mampu mengelola narasi publik secara efektif. Peran Kunci Komunikasi Strategis

1) Pembagian Informasi Intelijen yang Tepat Waktu. Serangan siber Tiongkok seringkali tersembunyi dan kompleks. Komunikasi strategis memungkinkan lembaga-lembaga ini untuk secara cepat dan aman berbagi intelijen mengenai ancaman yang terdeteksi.

2) Koordinasi Respons yang Terintegrasi. Ketika serangan siber terjadi, komunikasi strategis memastikan bahwa setiap lembaga tahu peran dan tanggung jawabnya. Ini mencegah tumpang tindih dan kebingungan.

3) Mengelola Narasi dan Disinformasi. Serangan siber dari Tiongkok sering kali disertai dengan kampanye disinformasi untuk menutupi jejak atau memecah belah publik.

c. Integrasi/keterpaduan. Pola integrasi kelembagaan yang dapat diterapkan dalam menanggulangi ancaman siber dari Tiongkok diantaranya dengan pembentukan satuan terpadu, tidak harus berarti peleburan total. Ada beberapa model yang bisa dipertimbangkan, seperti:

1) Pusat Komando Bersama (Joint Cyber Command): Sebuah badan kolaboratif yang terdiri dari perwakilan TNI dan Polri, namun masing-masing institusi tetap memiliki unit sibernya sendiri. Pusat ini bertugas sebagai koordinator utama untuk operasi siber berskala besar.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

2) Satuan Tugas Khusus (Task Force): Dibentuk saat ada kebutuhan mendesak atau ancaman spesifik. Dengan model seperti ini, kedua institusi tetap menjalankan tugas pokoknya, namun memiliki platform yang terstruktur untuk berbagi informasi, keahlian, dan sumber daya, terutama saat menghadapi ancaman siber yang kompleks seperti dari aktor negara.

b. Kapasitas Teknologi dan Infrastruktur dalam upaya Menanggulangi Ancaman Siber dari Tiongkok

Setelah revisi undang-undang No. 3 tahun 2025 terkait perubahan UU No. 34 tahun 2024 tentang TNI, pada revisi pasal 7 ayat 2 terkait tugas pokok OMSP TNI, ditambahkan poin 15 yang menyatakan salah satu tugas TNI bidang OMSP adalah membantu dalam upaya ancaman pertahanan siber. Hal ini sebagai pemberian legacy serta kesadaran dari pemerintah terkait ancaman masa kini dan dimasa yang akan datang tidak hanya pada peperangan terbuka. TNI memiliki kepentingan strategis dalam pertahanan siber di mana kondisi ancaman peperangan saat ini tidak hanya datang dari dunia nyata, namun dapat meluas ke dunia maya/siber.

Dihadapkan pada kapasitas TNI dalam penanggulangan ancaman siber dari Tiongkok, kondisi saat ini TNI telah memiliki satuan siber yang dapat dioperasionalkan pada upaya perlawanan siber terhadap negara/aktor non-negara yang dapat membahayakan pertahanan negara. Beberapa kemampuan satsiber saat ini terus dikembangkan dalam upaya memenuhi kebutuhan kompetensi TNI guna mengatasi ancaman ini. Salah satu kemampuan yang dibutuhkan adalah peralatan siber. Berdasarkan Permenhan No. 82 Tahun 2014 tentang Pertahanan Siber, alat teknologi (almatsus) sistem keamanan siber yang dimiliki TNI saat ini mencakup infrastruktur teknologi informasi dan komunikasi (TIK) yang dikembangkan untuk mendukung pertahanan siber, antara lain Cyber Operation Center (COC), sistem informasi yang terintegrasi, serta implementasi standar keamanan informasi berbasis SNI/ISO 27001. Selain itu, telah dibentuk Computer Security Incident Response Team (CSIRT) untuk menguji kesiapan dalam menghadapi serangan siber berskala besar. Teknologi ini masih dalam tahap pengembangan untuk mendukung kebutuhan pertahanan siber, termasuk dalam pengujian serangan siber, pengelolaan insiden, serta pengembangan sistem pengamanan informasi. Dihadapkan pada hasil penelitian terdahulu yang dilakasanakan oleh Andrea Angeline dkk (2023) yang berjudul “Profesionalisme TNI di Era Keamanan dan Pertahanan Siber Indonesia” bahwa profesionalisme institusi TNI, dari sisi pertahanan, sangat penting dalam merespons ancaman siber yang kompleks dan variatif dari segi aktor maupun motifnya.

Kemudian pada kompetensi yang dimiliki oleh instansi Polri, di mana instansi ini diberikan amanat sebagai penegak hukum, pelindung dan pengayom masyarakat sesuai amanat UU No. 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia. Dalam bidang ancaman siber, maraknya kejahatan siber (cyber crime) ditengah masyarakat, harus menjadi perhatian serius dalam penanggulangannya. Polri selama ini telah bersiap dalam mengatasi ancaman siber di mana penguatan kelembagaan melalui Ditipidsiber Bareskrim dan Bidinteltek Baintelkam. Penanganan kejahatan digital oleh Polri berfokus pada penyelidikan, penegakan hukum, dan edukasi publik, yang berkontribusi dalam membangun ketahanan siber masyarakat.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

Agar mampu menanggulangi ancaman siber dari Tiongkok yang semakin massive dan kuat, maka diperlukan pembangunan kapasitas TNI dan Polri dalam menanggulangi ancaman siber dari Tiongkok diarahkan pada peningkatan hasil kinerja.

a. Peningkatan kapasitas teknologi. Untuk mengatasi ancaman siber dari Tiongkok, diperlukan peningkatan teknologi yang berfokus pada pertahanan, deteksi dini, dan pemulihan. Peningkatan ini harus melampaui perangkat lunak dasar dan mencakup solusi canggih yang mampu menghadapi taktik spionase Tiongkok yang kompleks. Teknologi yang perlu ditingkatkan diantaranya: Sistem Pertahanan Berbasis Kecerdasan Buatan (AI) dan Pembelajaran Mesin (ML); Solusi Endpoint dan Extended Detection and Response (EDR/XDR); Teknologi Enkripsi dan Manajemen Kunci Kriptografi Lanjutan; Sistem Otentikasi Multifaktor (MFA) Kuat; Teknologi Enkripsi Kriptografi Kuantum; Forensik Digital dan Incident Response Lanjutan; Pengamanan Rantai Pasok Teknologi.

b. Peningkatan kapasitas infrastruktur. Untuk meningkatkan kemampuan satuan siber pada institusi TNI dan Polri maka perlu dilakukan penguatan pada dukungan infrastruktur yang lebih lengkap dan modern. Hal-hal yang perlu ditingkatkan dan ditambah meliputi: Regulasi dan kebijakan siber nasional memiliki peran krusial dalam membentuk sistem pertahanan siber yang tangguh, namun efektivitasnya sangat bergantung pada bagaimana kebijakan tersebut diimplementasikan, ditegakkan, dan diperbarui. Serta Penyediaan sarana prasarana berupa gedung, pusat data, Network Operation Center (NOC), laboratorium, dan fasilitas pendukung lainnya.

c. Strategi Kolaborasi TNI dan Polri yang Efektif guna Menanggulangi Ancaman siber

Setelah menguraikan kondisi sinergi dan kapasitas yang dimiliki oleh instansi TNI dan Polri dalam menanggulangi ancaman siber saat ini, maka hal penting yang harus dilaksanakan adalah meningkatkan kolaborasi antara TNI dan Polri, sehingga setiap ancaman siber dapat ditanggulangi secara kolaboratif.

Strategi disusun berdasarkan promises dan tujuan yang telah ditetapkan". Berdasarkan teori tersebut, maka strategi kolaborasi TNI dan Polri dalam menanggulngai ancaman dari Tiongkok dilaksanakan dengan penentuan aspek-aspek strategis yang kemudian dielaborasi untuk menghasilkan suatu strategi yang tepat sesuai kondisi yang terjadi dan dapat dibagi ke dalam lima tahapan utama yang saling melengkapi, diantaranya :

a. Tahap pertama dimulai dengan perumusan kebijakan dan regulasi yang kuat. Penguatan kerangka hukum nasional di bidang keamanan siber menjadi fondasi utama termasuk harmonisasi regulasi lintas sektor yang saat ini masih kerap tumpang tindih dan menghambat respons yang terkoordinasi. Selain itu, penyusunan standar nasional keamanan siber serta protokol penanganan insiden yang seragam dan adaptif harus menjadi fokus awal yang tak bisa ditunda. Hal ini dilaksanakan melalui revisi regulasi

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

dan penguatan kerangka hukum, khususnya terhadap UU ITE dan regulasi teknis lainnya, agar lebih adaptif terhadap dinamika dan modus baru serangan siber.

b. Tahap kedua menitikberatkan pada penguatan kapasitas dan kemampuan nasional. Sebagai contoh, pendirian Security Operation Center (SOC) yang terintegrasi di tingkat nasional sangat penting untuk mendeteksi dan merespons ancaman secara real-time. Selanjutnya dapat diselenggarakan melalui pembentukan badan Koordinasi Nasional Keamanan Siber. Pemerintah perlu membentuk badan koordinasi lintas lembaga yang terdiri dari unsur TNI, Polri, BSSN, BRIN, dan akademisi dari berbagai perguruan tinggi. Kolaborasi ini akan menciptakan pusat keunggulan (center of excellence) yang memadukan kemampuan strategis, teknis, dan akademik.

c. Tahap ketiga adalah pembangunan ekosistem kolaboratif lintas sektor. Keamanan siber bukan hanya tanggung jawab pemerintah, tetapi juga sektor swasta, akademisi, dan masyarakat sipil. Oleh karena itu, sinergi antar pemangku kepentingan mutlak diperlukan. Koordinasi antar lembaga seperti TNI, Polri, BSSN, dan Kementerian terkait perlu diperkuat. Koordinasi ini dapat dibangun melalui platform berbagi informasi yang bersifat cepat, transparan, dan responsif terhadap ancaman yang berkembang.

d. Tahap keempat berfokus pada peningkatan kesadaran dan edukasi publik. Program literasi keamanan siber nasional harus dirancang agar menjangkau seluruh lapisan masyarakat. Pelatihan rutin dan kampanye publik dapat menjadi benteng pertahanan awal yang sangat efektif dalam mencegah serangan siber di tingkat individu dan institusi. Tahap ini diselenggarakan untuk meningkatkan literasi siber dan melaksanakan edukasi massal secara sistematis. Masyarakat umum, termasuk pelajar dan pelaku Usaha Mikro, Kecil, dan Menengah (UMKM), perlu dibekali dengan pemahaman dasar mengenai prinsip-prinsip keamanan siber melalui kampanye edukatif berskala nasional yang berkelanjutan.

e. Tahap kelima adalah pengawasan dan evaluasi yang berkelanjutan. Setiap strategi perlu dikaji ulang secara periodik agar tetap relevan dengan perkembangan ancaman yang semakin kompleks. Pengembangan sistem peringatan dini yang handal juga perlu menjadi bagian dari sistem pertahanan nasional yang proaktif dan bukan reaktif.

Dihadapkan pada ancaman spesifik yang datang dari negara Tiongkok, maka strategi yang efektif dalam menanggulangi ancaman dapat dilaksanakan dengan kolaborasi antara TNI dan Polri (bersama instansi terkait) dapat ditingkatkan melalui beberapa strategi utama yaitu :

a. Pembentukan Pusat Komando Siber Nasional. Untuk meningkatkan koordinasi secara fundamental, dapat saja dibentuk sebuah Pusat Komando Siber Nasional yang berfungsi sebagai pusat koordinasi tunggal bagi seluruh lembaga terkait. BSSN saat ini dapat bertugas sebagai koordinator, sebuah pusat komando formal dengan perwakilan dari setiap lembaga (TNI dan Polri) dengan memastikan rantai komando yang jelas dan respons yang cepat saat terjadi insiden siber.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

b. Peningkatan Mekanisme Pertukaran Informasi. Pertukaran informasi yang cepat dan akurat adalah kunci. Koordinasi dapat ditingkatkan dengan membangun platform teknologi yang aman dan terpusat untuk berbagi intelijen siber dan laporan insiden secara real-time.

Dihadapkan pada upaya melindungi infrastruktur digital negara dari serangan siber Tiongkok adalah pendekatan berlapis, proaktif, dan terpadu. Strategi ini tidak hanya fokus pada teknologi, tetapi juga pada penguatan sumber daya manusia dan kolaborasi antarlembaga.

a. Penguatan Pertahanan Berlapis (Defense-in-Depth) Pendekatan ini mengadopsi konsep keamanan berlapis, di mana setiap lapisan memiliki mekanisme pertahanan sendiri.

b. Peningkatan Kemampuan Deteksi Dini dan Threat Intelligence daripada hanya menunggu serangan terjadi, penting untuk membangun kemampuan deteksi dini yang kuat.

Melalui strategi kolaborasi TNI dan Polri diharapkan dapat berperan sebagai landasan strategis dalam membentuk kerangka kolaboratif yang menyatukan berbagai lembaga dan badan yang bergerak di bidang keamanan siber di Indonesia. Selama ini, berbagai lembaga seperti TNI, Polri, BRIN, BSSN, dan peneliti di berbagai kampus bergerak sendiri-sendiri, tanpa adanya sinergi yang terpadu. Hal ini dapat menghambat efektivitas respons terhadap ancaman siber yang semakin kompleks. Oleh karena itu, kolaborasi yang terintegrasi ini diharapkan dapat berperan sebagai landasan strategis dalam membentuk kerangka kolaboratif yang menyatukan berbagai lembaga dan badan yang bergerak di bidang keamanan siber di Indonesia. Seluruh komponen bangsa yang mana setiap lembaga memiliki keunggulan masing-masing yang dapat saling melengkapi. TNI, misalnya, memiliki kekuatan dalam menghadapi ancaman siber yang bersifat geopolitik dan militer, sementara Polri lebih fokus pada penegakan hukum dan penanggulangan kejahatan siber yang bersifat kriminal. BRIN, dengan riset dan pengembangan teknologinya, dapat menyediakan solusi inovatif, sedangkan BSSN berfungsi sebagai koordinator nasional dalam kebijakan dan keamanan siber. Namun, selama ini, tiap lembaga ini bergerak secara terpisah, yang dapat menghambat efektivitas respons terhadap ancaman siber yang semakin kompleks dari negara Tiongkok.

5. KESIMPULAN DAN SARAN

a. Kesimpulan.

Kolaborasi TNI-Polri dalam menanggulangi ancaman siber sudah terbentuk dan mengarah pada perkembangan positif, namun dihadapkan pada ancaman siber yang datang dari negara Tiongkok memerlukan penguatan sinergi menghadapi kekuatan agresor yang dibekali kemampuan mutakhir. Ancaman serangan siber dari Tiongkok terus bertransformasi pada tingkat kompleksitas yang semakin kuat sebagai ancaman serius bagi stabilitas keamanan nasional. Hal tersebut memerlukan upaya kolaboratif antara TNI dan Polri dalam menanggulangi ancaman siber, sehingga melalui upaya sinergi dengan memadukan kerjasama, koordinasi dan integrasi yang efektif dapat

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

membentuk kekuatan pertahanan siber yang tangguh. Berbagai hambatan dan kendala selalu hadir dalam setiap upaya pencapaian tujuan, maka penting untuk memastikan kesiapan operasi, perencanaan aksi dan reformulasi kebijakan yang sesuai dengan kebutuhan dalam mengatasi ancaman di masa yang akan datang.

Strategi penanggulangan ancaman siber nasional harus dirancang secara menyeluruh dan bertahap untuk menciptakan integrasi aksi dan reaksi yang efektif antar unsur terkait. Strategi ini mencakup lima tahapan utama, yaitu: perumusan kebijakan dan regulasi yang kuat dan adaptif sebagai fondasi hukum kolaborasi lintas sektor; penguatan kapasitas dan kemampuan nasional melalui pembentukan badan koordinasi, pengembangan SDM, serta dukungan infrastruktur dan teknologi mutakhir; pembangunan ekosistem kolaboratif lintas sektor yang melibatkan pemerintah, swasta, akademisi, dan masyarakat; peningkatan kesadaran dan edukasi publik melalui literasi siber yang masif dan sistematis sejak dini; serta pengawasan dan evaluasi berkelanjutan untuk memastikan strategi selalu relevan menghadapi dinamika ancaman siber yang semakin kompleks dan canggih. Pendekatan bertahap ini menjadi kunci dalam membentuk ketahanan siber nasional yang adaptif, responsif, dan berkelanjutan.

b. Saran. Saran yang ditujukan bagi pelaksanaan praktis guna menanggulangi ancaman siber dari negara Tiongkok melalui kolaborasi antara TNI dan Polri yaitu dengan:

1) Presiden bersama DPR segera menuyusun Undang-undang Keamanan Nasional dihadapkan pada kepentingan mengatasi transformasi ancaman keamanan negara yang semakin kompleks dan multidimensi, dengan memuat pengaturan tentang penanggulangan ancaman siber secara terpadu. Melalui regulasi ini, pemerintah menegaskan perlunya integrasi lintas sektor dengan melibatkan seluruh unsur kekuatan nasional, serta lembaga strategis lainnya dalam satu kerangka sistem pertahanan dan keamanan siber nasional.
2) BSSN segera membentuk platform kolaborasi permanen melalui pembentukan satuan terpadu berbasis kan Cyber Security Command Center yang bersifat lintas sektoral untuk mewujudkan gelar operasi terpadu pengamanan siber dalam negeri dengan leading sector institusi TNI dan Polri sesuai tugas pokok dan kewenangannya.
3) Panglima TNI dan Mabes Polri membentuk suatu regulasi Role of Engagement untuk melibatkan instansi satu sama lainnya dalam menanggulangi ancaman siber dalam bidang masing-masing sesuai ketentuan dan kewenangan konstitusinya (TNI bidang pertahanan dan Polri bidang keamanan).
4) Panglima TNI bersama Kementerian Pertahanan membentuk tim internal melaksanakan evaluasi dan analisis pembangunan kapasitas TNI dalam menanggulangi ancaman siber. Kemudian mengajukan anggaran kepada pemerintah guna pembangunan kekuatan siber TNI yang ideal dalam menanggulangi ancaman siber saat ini dan di masa yang akan datang.
5) Kapolri membentuk tim internal melaksanakan evaluasi dan analisis pembangunan kapasitas Polri dalam menanggulangi ancaman siber. Kemudian mengajukan anggaran kepada pemerintah guna pembangunan kekuatan siber Polri yang ideal dalam menanggulangi ancaman siber.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

DAFTAR PUSTAKA

Arthur Lykke. (1993) Military Strategy: Theory and Aplication. Pennsylvania: US Army War College

Al A'raf, (2015) Dinamika Keamanan Nasional. Jurnal Keamanan Nasional Vol 1 (1) tahun 2015.

Agus Subagyo (2015) "Sinergi dalam menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat. Jurnal Pertahanan Vol 5 nomor 1 tahun 2015.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of

Apriyani, L., Purwanto, S., & Bimo, W. A. (2024). Pengaruh Motivasi Kerja Dan Disiplin Kerja Terhadap Kinerja Karyawan Pada Pt. Istana Garmindo Jaya. *Jurnal Ekonomi dan Bisnis Digital*, *2*(1), 622-629.

Alam, S., Sutanto, R., & Purwanto, S. (2025). Analisis Efektifitas Kerjasama TNI-Polri untuk Menangani Destructive Fishing Guna Mendukung Ekonomi Biru dalam Rangka Pembangunan Nasional. *Jurnal Pendidikan Indonesia*, *6*(11), 4833-4845.

Barry Buzan, (1991) People, States and Fear: an Agenda for International Security Studies in the Post-Cold War. Boulder: Lynne Rienner Publisher, 19.

Baron, Robert A., Donn Erwin Byrne (2000) Social Psychology. 9th Edition. Pinted In The United State Of America

Bambang Darmono, (2010) "Konsep dan Sistem Keamanan Naional Indonesia" Yogyakarta : Jurnal Ketahanan Nasional. Vol. 15 No. 1 tahun 2010.

Barki, H., & Pinsonneault, A. (2005). A model of organizational integration, implementation effort, and performance. Organization Science, 16(2), 165–179. http://dx.doi.org/10.1287/orsc.1050.0118

Boothby, W. H. (2013). Methods and Means of Cyber Warfare. International Law Studies, 89, 387–405.

Boston R Sihotang, dkk (2021) Optimalisasi Sinergitas TNI-Polri Dalam Penanggulangan Terorisme di Indonesia. Jurnal Ilmu Administrasi Negara. Vol No. 9 tahun 2021

Covey, Steven R. (2010). The 7 Habits of Highly Effective People (7 Kebiasaan Manusia yang Sangat Efektif). Tangerang: Binarupa Aksara Publisher.

CISA. (2024). People's Republic of China Cyber Threat Overview and Advisories. Cybersecurity and Infrastructure Security Agency. Online di : https://www.cisa.gov/ diakses pada 10 Oktober 2025

David, Fred. R.(2011) "Manajemen Strategis:Konsep-Konsep." Jakarta: PT.Indeks.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

Dr. Priyanto, S.IP., M.Si. Han (2024) "Network Centric Warfare (NCW) dalam perspektif manajemen pertahanan negara" Jakarta : CV. Aksara Global Akademia.

Efriza. 2012. Political Explore: Sebuah Kajian Ilmu Politik. Jakarta: Alfabeta.

Gray, Barbara, (1989) Collaborating: Finding Common Ground Formultiparty Problems. San Francisco, CA:Jossey-Bass.

Grace B. Mueller, et all (2023) Cyber Operations during the Russo-Ukrainian War. online di: https://www.csis.org/ diakses pada 27 Maret 2025

Hasibuan, H. Malayu S.P. (2006). Manajemen Sumber Daya Manusia (Edisi Revisi). Jakarta: Bumi Aksara.

Husein Umar (2013) Desain Penelitian Manajemen Strategik, Jakarta: Rajawali Pers.

Ineu Rahmawati (2017) Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. Jurnal Pertahanan & Bela Negara. Vol. 7 No. 2 Tahun 2017

Keio, A., Suhirwan, & Dohamid, A. G. (2025). Ancaman perang siber China terhadap Indonesia: Analisis strategi, dampak, dan respons kebijakan. Universitas Pertahanan Republik Indonesia. Rayyan Jurnal Ilmiah Aurelia, 5(2), 45–58.

Miles, M.B, Huberman, A.M, & Saldana, J. (2014) Qualitative Data Analysis, A Methods Sourcebook, Edition 3 (Terjemahan Tjetjep Rohindi Rohidi) Jakarta : UI-Press.

Muhammad Hatim, dkk (2024) Upaya Meningkatkan Pertahanan Negara Dari Ancaman Siber Melalui Strategi Pengembangan Senjata Siber di Indonesia. Nusantara: Jurnal Ilmu Pengetahuan Sosial. Vol. 11 (1) tahun 2024.

Nur Arifina, (2022) Pertahanan siber Indonesia di Kementerian Pertahanan Republik Indonesia. Jurnal Peperangan Asimetris. Vol. 8 No. 1 tahun 2022.

O'Flynn, J., & Wanna, J. (2008). Collaborative Governance : A new era of public policy in Australia? Canberra, ACT, Australia: ANU ePress.https://doi.org/10.26530/oapen_458884

Parks, P. J. (2013). Cyberwarfare. San Diego : Reference Point Press

Prasetiawan, H. P., AR, D. D., & Purwanto, S. (2025). THE STRATEGY TO IMPROVE THE CHARACTER OF MILITARY ACADEMY CADETS THROUGH THE ROLE OF MENTORS IN SHAPING PROFESSIONAL OFFICERS TO SUPPORT THE MAIN DUTIES OF THE INDONESIAN ARMY. *Santhet (Jurnal Sejarah Pendidikan Dan Humaniora)*, *9*(6), 2184-2191.

Purwanto, S., & Siagian, F. (2025). Strategic human resources management in the global era: Navigating opportunities and challenges. *Centurion MSPD Journal*, *1*

Purwanto, S., Wibowo, A., & Suharti, T. (2023). The OCB Determinant of Employees in Non-Profit Organization; Leadership Role and Work Engagement. *inovator*, *12*(2), 251-263.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 2
NOVEMBER 2025

Purwanto, S., Supangat, S., Esterina, M., Souhoka, S., Chandra, F., Hariputra, A., ... & Arianto, T. (2024). *Manajemen sumber daya manusia*. Yayasan Tri Edukasi Ilmiah.

Ratna, Nyoman Kutha. (2012) Penelitian Sastra: Teori, Metode, dan Teknik. Yogyakarta: Pustaka Pelajar.

Sekoia. (2023). A Three-Beat Waltz: The Ecosystem Behind Chinese State-Sponsored Cyber Threats. Sekoia Threat Intelligence.

Sugiyono (2017) Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: CV. Alfabeta

The Record. (2023). Indonesian intelligence agency compromised in suspected Chinese hack. Recorded Future News. Oline di https://therecord.media/ diakses pada 10 Oktober 2025

Undang-undang RI No. 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia

Undang-undang RI No. 3 tahun 2003 tentang Pertahanan Negara

Undang-undang RI No. 3 tahun 2025 tentang Perubahan Undang-undang No. 34 tahun 2004 tentang Tentara Nasional Indonesia

Peraturan Pemerintah No. 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Presiden No. 66 tahun 2019 tentang Susunan Organisasi Tentara Nasional Indonesia.

Pace dan Faules (2005) Organizational Communication. Englewood Cliffs, NJ: Prentice Hall.

Walton, J. (1999) Strategic Human Resource Development. Edinburg : Pearson Education Limited.