KOMISI I
Pertahanan, Luar Negeri, dan Informatika

Analisis Strategis terhadap Isu Aktual
INFO Singkat

VOL. XVII, NO. 15/I/PUSAKA/AGUSTUS/2025

# PERAN TNI DALAM KEAMANAN SIBER: PERLUKAH PEMBENTUKAN ANGKATAN SIBER?

Aulia Fitri*

Abstrak

*Wacana pembentukan Angkatan Siber TNI kembali mengemuka pasca kesepakatan kerja sama keamanan siber antara Indonesia dan Singapura. TNI telah memiliki satuan siber yang dibentuk sejak tahun 2017, sedangkan Singapura membentuk angkatan siber sebagai matra ke-4 pada tahun 2022. Menteri Pertahanan RI menyatakan bahwa saat ini belum perlu membentuk matra baru. Tulisan ini membahas peran TNI dalam keamanan siber serta memberikan ulasan mengenai perlu atau tidaknya pembentukan angkatan siber. Meskipun terdapat urgensi strategis penguatan pertahanan siber, penguatan Satuan Siber TNI yang sudah terbentuk dapat menjadi pendekatan yang lebih implikatif dibandingkan dengan pembentukan angkatan baru yang membutuhkan penataan ulang organisasi, alokasi anggaran, serta penyesuaian terhadap kebijakan pertahanan nasional. Melalui fungsi pengawasan, Komisi I DPR RI dapat mendorong Panglima TNI untuk meningkatkan kapabilitas Satuan Siber TNI melalui pengembangan SDM, dukungan teknologi, serta memperkuat koordinasi dengan kementerian/lembaga terkait. Selain itu, kerja sama internasional di bidang keamanan siber juga perlu ditingkatkan melalui diplomasi pertahanan.*

## Pendahuluan

Wacana pembentukan Angkatan Siber Tentara Nasional Indonesia (TNI) muncul kembali pasca kesepakatan kerja sama keamanan siber antara Indonesia dan Singapura. Namun, Menteri Pertahanan Sjafrie Sjamsoeddin menyatakan bahwa saat ini TNI belum memerlukan angkatan siber sebagai matra ke-4 TNI (Harahap, 2025). Ancaman keamanan telah mengalami pergeseran, dari ancaman yang bersifat konvensional menjadi ancaman yang bersifat asimetris, salah satunya ancaman siber. Ruang siber merupakan sektor yang bersifat kompleks karena memiliki interkonektivitas dengan sektor-sektor lainnya. Fenomena seperti *cyber warfare*, *cyber espionage* hingga *cyber terrorism* menjadi tantangan nyata yang dapat mengancam keamanan negara (Darumaya dkk, 2023).

Tentara Nasional Indonesia (TNI) sebagai komponen utama pertahanan negara telah beradaptasi dalam merespons ancaman siber melalui pembentukan Satuan Siber TNI sejak

*) Analis Legislatif Ahli Muda Bidang Politik, Hukum, Keamanan, dan HAM pada Pusat Analisis Keparlemenan, Badan Keahlian DPR RI. *Email: aulia.fitri@dpr.go.id.*

tahun 2017. Wacana mengenai pembentukan angkatan siber sebagai matra keempat TNI juga sempat beberapa kali mengemuka. Pertama, ketika terjadi serangan *ransomware* terhadap Pusat Data Nasional pada tahun 2024 (Nugroho, 2024). Kedua, pada kesepakatan kerja sama keamanan siber antara Kementerian Pertahanan Indonesia dan Singapura tahun 2025 (Harahap, 2025). Namun demikian, menurut Menteri Pertahanan Sjafrie Sjamsoeddin, wacana pembentukan angkatan siber tersebut belum diperlukan (Septianto, 2025). Penguatan kemampuan siber dipandang sebagai sebuah kebutuhan, namun pembentukan matra baru bukan merupakan keputusan sederhana karena terkait dengan struktur organisasi, anggaran, sumber daya dan kebijakan pertahanan nasional. Tulisan ini membahas peran TNI dalam menghadapi ancaman siber termasuk memberikan gambaran mengenai perlu atau tidaknya pembentukan angkatan siber dalam organisasi TNI.

## Peran TNI dalam Menghadapi Ancaman Siber

Ancaman keamanan siber telah berkembang pesat dan turut memengaruhi dinamika lingkungan strategis. Dampak ancaman siber terhadap kepentingan nasional juga diakui oleh Perserikatan Bangsa-Bangsa (PBB) sehingga muncul seruan agar negara membangun pertahanan siber nasional (United Nations, 2021). Jauh sebelum seruan tersebut, TNI telah membentuk Satuan Siber pada tahun 2017. Satuan Siber TNI dibentuk sebagai respons terhadap tantangan keamanan siber yang semakin kompleks. Satuan ini terdiri dari gabungan ketiga matra TNI dan bertugas menyelenggarakan kegiatan dan operasi siber di lingkungan TNI dalam mendukung tugas pokok TNI. Dengan kemampuan untuk mendeteksi, merespons, dan mengedukasi, Satuan Siber TNI bukan hanya melindungi infrastruktur kritis, tetapi juga berkontribusi terhadap ketahanan siber nasional (Fitriati, 2018). Meski demikian, masih terdapat beberapa kendala yang dialami oleh Satuan Siber TNI, di antaranya kurangnya jumlah personil dengan keahlian keamanan siber, serta teknologi dan infrastruktur yang belum mutakhir (Hadi, 2021). Selain itu, masih diperlukan peningkatan sinergi dan integrasi antara satuan siber TNI dengan BSSN, Polri, serta instansi pemerintah lain untuk memperkuat efektivitas penanganan ancaman siber secara lebih optimal (Sari & Pratama, 2022).

Peranan TNI di ranah siber juga telah didukung secara regulasi melalui Undang-Undang No. 3 Tahun 2025 tentang Perubahan atas Undang-Undang No. 34 Tahun 2004 tentang Tentara Nasional Indonesia yang mencantumkan penanggulangan ancaman siber dalam tugas pokok operasi militer selain perang. Dalam konteks ini, peran TNI di ruang siber akan relevan dengan perkembangan lingkungan strategis dengan fokus utama *cyber warfare* dan *cyber defense*. Secara lebih spesifik, TNI akan menanggulangi penyerangan terhadap sistem pertahanan dan komando militer di ruang siber dengan bentuk ancaman berupa peretasan, sabotase digital, atau pencurian data strategis. TNI juga akan menanggulangi ancaman terhadap infrastruktur kritis nasional seperti serangan terhadap jaringan listrik dan telekomunikasi. Selain itu, TNI juga akan menanggulangi serangan siber dari aktor negara atau non-negara yang berdampak pada keamanan nasional berupa *cyber espionage* maupun *cyber warfare* (Indonesiadefense, 2025).

TNI memiliki peran penting dalam menghadapi serangan siber yang berpotensi mengancam pertahanan negara, baik dari segi keamanan nasional maupun operasional militer. Hal ini menjadi kebutuhan strategis bagi Indonesia di tengah transformasi global, di mana bentuk peperangan modern tidak lagi terbatas pada aktivitas fisik di suatu wilayah. Saat ini, peperangan telah bergeser ke ranah siber yang melibatkan sabotase digital, pencurian data intelijen, dan konflik geopolitik (Fox, 2024).

## Upaya Peningkatan Kapabilitas Siber TNI

Munculnya wacana pembentukan Angkatan Siber TNI kembali mengemuka setelah Kementerian Pertahanan Indonesia dan Singapura menyepakati kerja sama keamanan siber pada bulan Juli 2025. Indonesia berencana untuk belajar dan bertukar informasi dari pengalaman Singapura yang membentuk angkatan siber pada tahun 2022. Sebelumnya, wacana ini juga pernah mengemuka pasca terjadinya serangan siber terhadap Pusat Data Nasional pada tahun 2024. Pada pertemuan lanjutan Menteri Pertahanan (Menhan) kedua negara pada 5 Agustus 2025, Menhan RI Sjafrie Sjamsoeddin menyatakan bahwa TNI belum perlu membentuk Angkatan Siber secara terpisah karena TNI sudah memiliki satuan siber sendiri yang dapat dikolaborasikan dengan elemen sipil dalam kerangka pertahanan semesta (Faturrahman, 2025). Indonesia menganut konsep Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) yang menekankan pentingnya kolaborasi kedua unsur militer dan sipil dalam pertahanan nasional (Kementerian Pertahanan, 2015).

Wacana pembentukan Angkatan Siber dan eksistensi Satuan Siber TNI dapat dipahami sebagai respons terhadap ancaman siber yang semakin nyata, contohnya serangan *ransomware* server Pusat Data Nasional (PDN) yang berdampak pada data milik Badan Intelijen Strategis (BAIS) TNI yang diretas dan diperjualbelikan di *dark web* (Dewi, 2024). Selain kasus di atas, terdapat beberapa kasus terkait siber lainnya yang pernah terjadi di Indonesia, seperti peretasan situs Komisi Pemilihan Umum (KPU) pada Pemilihan Kepala Daerah (Pilkada) Serentak tahun 2018, kasus *ransomware wannacry* tahun 2018 yang melumpuhkan sistem komputer beberapa rumah sakit dan perusahaan besar di Jakarta, dan kasus penyadapan komunikasi pribadi Presiden RI pada tahun 2013 oleh Australia, berdasarkan dokumen yang dibocorkan oleh Edward Snowden, mantan anggota National Security Agency Amerika Serikat. Selain itu, terdapat juga kasus *cyber terrorism*, penyalahgunaan internet oleh kelompok jaringan teroris Imam Samudra untuk menyebarkan propaganda, paham-paham radikal, melakukan *hacking*, *cracking*, dan *carding* untuk mengumpulkan dana dan melakukan rekrutmen anggota (Hadi, 2021).

Menghadapi ancaman yang terus berkembang, pembangunan kekuatan siber menjadi penting untuk memperkuat ketahanan nasional serta kapabilitas pertahanan dan keamanan negara. Ruang siber telah menjadi medan perang yang tidak terlihat tetapi memiliki dampak yang signifikan. Dampak peperangan siber tidak dapat dipandang sebelah mata. Melalui serangan siber, suatu negara dapat dilumpuhkan dari sisi ekonomi

melalui serangan ke sektor perbankan dan finansial. Dari sisi infrastruktur, serangan siber juga dapat melumpuhkan fasilitas telekomunikasi, energi, dan transportasi, termasuk sektor administrasi pemerintahan. Apabila serangan siber diluncurkan sebelum serangan militer, maka suatu negara akan dengan mudah dikuasai.

Serangan melalui media siber tanpa menghadirkan kekuatan militer secara fisik di negara lawan telah menjadi tren baru dalam peperangan modern. Oleh karena itu, upaya TNI dalam memperkuat kapabilitas pertahanan siber menjadi sebuah urgensi, mengingat TNI juga memiliki potensi besar dalam pengembangan kemampuan siber, seperti struktur komando yang solid, kedisiplinan organisasi, dan kemampuan operasional strategis yang dapat dimanfaatkan dalam konteks pertahanan siber nasional.

Meskipun terdapat urgensi strategis dalam memperkuat pertahanan siber nasional, pembentukan angkatan siber sebagai matra baru bukanlah satu-satunya pendekatan yang efektif. Pendekatan tersebut memerlukan reformasi struktural yang menyeluruh, mencakup penataan ulang organisasi, alokasi anggaran yang signifikan, serta penyesuaian terhadap kebijakan pertahanan nasional. Pendekatan yang lebih implementatif adalah penguatan Satuan Siber TNI yang sudah ada di dalam organisasi TNI. Penguatan yang dapat dilakukan di antaranya melalui peningkatan kapasitas personel, modernisasi infrastruktur dan teknologi, serta peningkatan koordinasi antarlembaga terkait seperti Badan Sandi dan Siber Negara (BSSN), Kementerian Pertahanan, POLRI, dan BIN.

## Penutup

Peran TNI dalam penanggulangan keamanan siber terlihat dari komitmen TNI dalam membentuk dan menjalankan Satuan Siber TNI. Pemberian ruang yang lebih luas bagi TNI untuk dapat menangani ancaman keamanan siber juga didukung dalam Undang-Undang tentang TNI melalui penambahan tugas pokok dalam operasi militer selain perang. Upaya peningkatan kapabilitas penanganan keamanan siber juga muncul dari wacana pembentukan matra siber TNI, sebagai respons terhadap dinamika ancaman siber yang semakin kompleks. Namun demikian, penguatan terhadap Satuan Siber TNI yang sudah terbentuk dapat menjadi pendekatan yang lebih implementatif daripada membentuk matra baru.

Melalui fungsi pengawasan, Komisi I DPR RI dapat menghimbau Panglima TNI untuk meningkatkan kapabilitas Satuan Siber TNI baik dari sisi pengembangan keahlian personel maupun dukungan infrastruktur teknologi. Komisi I DPR RI juga dapat mendorong Satuan Siber TNI untuk meningkatkan kerja sama dan koordinasi antarlembaga terkait seperti BSSN, BIN, dan Kementerian Pertahanan. Selain itu, upaya diplomasi pertahanan juga dapat ditingkatkan, khususnya melalui kerja sama di bidang keamanan siber.

## Referensi


- Darumaya, B., Maarif, S.,Toruan., Swastanto, Y. (2023). Pemikiran potensial ancaman perang siber di Indonesia: Suatu kajian strategi pertahanan. *Jurnal Keamanan Nasional*, Vol. IX No. 2. pp. 299-324.
- Dewi, S. (2024). TNI cek dugaan bocornya data BAIS di *dark web*. *IDN Times*. https://www.idntimes.com/news/indonesia/tni-cek-dugaan-bocornya-data-bais-di-dark-web-00-bbwlv-bk0tl8
- Harahap, D. (2025). Indonesia dan Singapura perkuat kerjasama militer keamanan siber. *Media Indonesia*. https://mediaindonesia.com/politik-dan-hukum/793988/indonesia-dan-singapura-perkuat-kerjasama-militer-keamanan-siber
- Faturrahman, A. (2025). Menteri Pertahanan: TNI tak perlu membentuk angkatan siber. *Tempo*. https://www.tempo.co/politik/menteri-pertahanan-tni-tak-perlu-membentuk-angkatan-siber-2055238
- Fitriati, R. (2018). *Membangun model kebijakan nasional keamanan siber dalam sistem pertahanan negara*. Jakarta: Universitas Pertahanan Indonesia.
- Fox, C. A. (2024). The principles for the future of warfare and stand-off warfare. *Association of the United States Army*. https://www.ausa.org/publications/principles-future-warfare-and-stand-warfare
- Hadi, R. (2021). Peran TNI dalam keamanan siber: Tantangan dan peluang. *Jurnal Pertahanan & Keamanan*, Vol.7(2). pp 45-58.
- Indonesia Defense. (2025). Kemhan beberkan bentuk ancaman siber yang akan ditangani TNI. *Indonesia Defense Magazine*. https://indonesiadefense.com/kemhan-beberkan-bentuk-ancaman-siber-yang-akan-ditangani-tni/
- Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia 2015*. Jakarta: Kementerian Pertahanan RI.
- Nugroho, N. P. (2024). Kapuspen sebut wacana pembentukan angkatan siber TNI masih digodok. *Tempo*. https://www.tempo.co/hukum/kapuspen-sebut-wacana-pembentukan-angkatan-siber-tni-masih-digodok--43632
- Septianto, B. (2025). Menhan nilai Indonesia belum butuh bentuk angkatan Siber di TNI. *Tirto.id*. https://tirto.id/menhan-nilai-indonesia-belum-butuh-bentuk-angkatan-siber-di-tni-hfm6
- United Nations. (2021). Cyberconflicts and National Security. United Nations. https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security.




*© 2009*

*Hak cipta dilindungi oleh undang-undang. Dilarang mengutip atau memperbanyak sebagian atau seluruh isi tulisan ini tanpa izin penerbit.*