Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 378-382

STRATEGI NASIONAL DEMI MENGHADAPI TERORISME SIBER DITINJAU DARI PERATURAN MENTERI PERTAHANAN NOMOR 82 TAHUN 2014

Fika Tantri Amaliah
[1,2] *Uin Sunan Gunung Djati Bandung, Indonesia*
*Correspondence: fikatantri2@gmail.com

Abstract (English)

This study aims to provide knowledge and to describe the results of the author's research on the national strategy for dealing with cyber terrorism in terms of the Minister of Defense Regulation number 82 of 2014. The method used in this research is normative juridical, namely law that is conceptualized as the name of a norm, rule, principle or dogma. -dogma. This approach is also known as the normative or doctrinal approach or research. The normative juridical research stage is carried out through a literature study (literature study) examining the literature. The results of this study are: Cyber terrorism is a strategic issue that currently needs attention. All lines of sectors, both private and government, must be able to view this problem as a whole because the impact of this problem is related to the astagatra aspects of Indonesia's national resilience. In the context of preparation, development, development and implementation of cyber defense within the Ministry of Defense or TNI, it is necessary to have a common understanding of the principles, objectives and tasks, roles and functions of cyber defense to be carried out. This becomes a reference in determining the risks posed so as to determine the cyber defense steps to be taken.

Article History
Submitted: 18 November 2024
Accepted: 21 November 2024
Published: 28 November 2024

Keywords:
Strategy; Cyber Terrorism; PERMENHAN.
.

Abstrak (Indonesia)

Penelitian ini bertujuan untuk menjadi pengatahuan dan mendeskrisikan mengenai hasil penelitian penulis tentang strategi nasional demi menghadapi terorisme siber ditinjau dari peraturan menteri pertahanan nomor 82 tahun 2014. Metode yang digunakan dalam menelitian ini yuridis normatif yaitu hukum yang dikonsepkan sebagainama sebuah norma, kaidah, asas ataupun dogma-dogma. Pendekatan ini dikenal pula dengan istilah pendekatan atau penelitian normatif atau dokrinal. Tahap penelitian yuridis normatif dilakukan melalui studi kepustakaan *(study literature)* menelaah terhadap literatur. Hasil dari penelitian ini yaitu : Terorisme siber adalah isu strategis yang saat ini perlu menjadi perhatian. Semua lini sektor, baik swasta maupun pemerintah, harus dapat memandang masalah ini secara menyeluruh karena dampak dari masalah ini berkenaan dengan aspekaspek astagatra ketahanan nasional Indonesia. Dalam rangka persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan atau TNI, diperlukan persamaan pemahaman tentang prinsip-prinsip, sasaran serta tugas, peran dan fungsi pertahanan siber yang akan dilaksanakan. Hal ini menjadi acuan dalam penetapan resiko yang ditimbulkan sehingga menentukan langkah-langkah pertahanan siber yang akan diambil.

Sejarah Artikel
Submitted: 18 November 2024
Accepted: 21 November 2024
Published: 28 November 2024

Kata kunci:
Strategi; Terorisme Siber; PERMENHAN.

Pendahuluan

Munculnya teknologi telah membawa kemajuan yang signifikan dalam kehidupan kita sehari-hari, tetapi dengan kemajuan ini muncul risiko dan ancaman baru. Terorisme siber, yang mengacu pada penggunaan teknologi untuk melakukan aksi terorisme, menjadi perhatian yang semakin meluas di dunia digital yang saling terhubung saat ini. Hal ini dapat menimbulkan ancaman bagi individu dan organisasi, dengan konsekuensi potensial mulai dari informasi pribadi yang disusupi hingga gangguan sistem yang meluas atau bahkan bahaya fisik.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 378-382

Menurut berbagai laporan, motivasi di balik terorisme siber mencakup alasan politik dan ideologis, keuntungan finansial, atau sekadar niat jahat. Konsekuensi dari terorisme siber bisa parah dan berjangkauan luas, berpotensi menyebabkan kepanikan dan ketidakstabilan yang meluas. Pemerintah, badan keamanan, dan ahli komputer di seluruh dunia bekerja untuk menangkal terorisme dunia maya melalui berbagai cara seperti peningkatan langkah-langkah keamanan digital, sistem pengawasan canggih, dan teknik penambangan data (Fujiyama, 2022).

Namun, kompleksitas dan sifat ancaman dunia maya yang terus berkembang membuat tugas ini menantang. Yang penting, beberapa penulis yang tidak menganggap terorisme siber sebagai ancaman yang signifikan percaya bahwa penanggulangan tetap diperlukan untuk menjaga dari risiko yang ditimbulkan oleh cyberwarfare dan cybercrime yang menurut mereka memang menimbulkan ancaman yang signifikan. Akibatnya, pertanyaan tanggapan menjadi kompleks dalam konteks ini, membutuhkan keseimbangan antara kepentingan publik dalam melindungi infrastruktur kritis dan naluri memaksimalkan keuntungan dari sektor swasta.

Sesuai dengan definisi yang diberikan oleh U.S. Federal Bureau of Investigation, terorisme siber mengacu pada setiap tindakan bermotivasi politik yang bertujuan untuk menyerang sistem informasi dengan maksud menyebabkan kerusakan pada target non-kombatan atau menciptakan ketidakstabilan. Untuk menangkal terorisme dunia maya secara efektif, pemerintah harus mempertahankan tindakan pencegahan yang memadai terhadap berbagai bentuk ancaman dunia maya, termasuk perang dunia maya dan kejahatan dunia maya. Penanggulangan ini sering melibatkan langkah-langkah keamanan digital, sistem pengawasan, dan teknik penambangan data untuk mendeteksi dan merespons potensi ancaman secara real-time. Namun, mengingat bahwa ancaman dunia maya sangat kompleks dan terus berkembang, mengembangkan penanggulangan yang efektif menghadirkan tantangan yang signifikan. Oleh karena itu, sangat penting bagi pemerintah untuk melakukan penilaian rutin terhadap sistem dan jaringan keamanan siber mereka dan terus memantau kemajuan teknologi (Okti, 2020).

Selain itu, karena sifat sistem digital kita yang saling terhubung, kerja sama internasional juga penting dalam menangani terorisme siber. Kolaborasi antara pemerintah, entitas swasta, dan organisasi internasional sangat penting untuk mengembangkan pendekatan terkoordinasi yang dapat mengatasi masalah terorisme siber secara efektif. Namun, tugas ini diperumit oleh persaingan kepentingan antara perusahaan swasta dan lembaga publik.

Kemudian, munculnya terorisme siber sebagai ancaman yang signifikan menyoroti perlunya lembaga pemerintah dan organisasi swasta untuk berkolaborasi dalam mengembangkan tindakan pencegahan yang kuat yang memperhitungkan sifat berkembang dari ancaman dunia maya baru. Dengan demikian, sangat penting bagi semua pemangku kepentingan untuk mengadopsi pendekatan proaktif untuk mengatasi masalah terorisme siber dan menerapkan tindakan pencegahan yang diperlukan yang dapat secara efektif mengurangi potensi ancaman dan melindungi infrastruktur digital yang penting.

Masalah terorisme siber adalah hasil dari meningkatnya penggunaan teknologi dalam kehidupan kita sehari-hari, dan konsekuensinya dapat berkisar dari informasi pribadi yang dikompromikan hingga kerusakan fisik, menyoroti perlunya kewaspadaan berkelanjutan dan langkah-langkah proaktif untuk mengatasi ancaman ini. Atas permasalahan tersebut penulis membuat jurnal tentang **"Strategi Nasional Demi Menghadapi Terorisme Siber Ditinjau Dari Peraturan Menteri Pertahanan Nomor 82 Tahun 2014".**

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 378-382

Metodologi

Metodologi penelitian yang merupakan prosedur untuk memperoleh pengetahuan yang benar melalui langkah-langkah yang sistematis. Sementara itu, dengan bertolak dari topik yang diangkat penelitian ini menggunakan metode pendekatan yuridis normatif yaitu hukum yang dikonsepkan sebagainama sebuah norma, kaidah, asas ataupun dogma-dogma. Pendekatan ini dikenal pula dengan istilah pendekatan atau penelitian normatif atau dokrinal. Tahap penelitian yuridis normatif dilakukan melalui studi kepustakaan *(study literature)* menelaah terhadap literatur. (zaenal arifin, 2017).

Studi kepustakaan ini dapat menyajikan analisis ilmiah yang berdasar terhadap kaidah keilmuan. Dalam penelitiannya penulis merujuk kepada jurnal ilmiah, buku-buku, peraturan perundang-undangan dan artikel yang relevan. Tekhnik pengumpulan data yang digunakan menurut Ahmad Tanzeh, pengumpulan data yang sistematik dan standar untuk memperoleh data yang diperlukan. Mula-mula mencari sumber dan data dari buku-buku, jurnal ilmiah dan lain sebagainya. Kemudian dikumpulkan sebagai bahan dan disajikan kedalam bentuk tulisan ilmiah (Ahmad Tanzeh, 2011).

Hasil dan Pembahasan

Terorisme siber adalah isu strategis yang saat ini perlu menjadi perhatian. Semua lini sektor, baik swasta maupun pemerintah, harus dapat memandang masalah ini secara menyeluruh karena dampak dari masalah ini berkenaan dengan aspekaspek astagatra ketahanan nasional Indonesia. Salah satu prinsip penanggulangan terorisme adalah peningkatan core value (nilai pokok). Hal ini berkaitan dengan asas kekeluargaan dalam ketahanan nasional yang mengutamakan prinsip perbedaan dan tanggung jawab bersama. Implementasi aktivitas kerjasama ini contohnya adalah neighbourhood watch group. Aktivitas ini melibatkan masyarakat atau warga dalam melakukan tindakan pre-emptive seperti pengawasan dan pengamanan secara bersama terhadap potensi kejahatan atau aksi teror di lingkungan sekitar (Bambang, 2017).

Pokok-pokok pertahanan siber

Dalam rangka persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan atau TNI, diperlukan persamaan pemahaman tentang prinsip-prinsip, sasaran serta tugas, peran dan fungsi pertahanan siber yang akan dilaksanakan. Hal ini menjadi acuan dalam penetapan resiko yang ditimbulkan sehingga menentukan langkah-langkah pertahanan siber yang akan diambil.

Prinsip-prinsip Pertahanan Siber yaitu diantaranya : *Pertama*, memiliki model pengamanan informasi yang terstruktur dan terintegrasi serta mengadopsi berbagai standar dan panduan pengamanan informasi yang ditetapkan oleh institusi yang berwenang. *Kedua,* faktor kerahasiaan, integritas dan ketersediaan pertahanan siber harus dipastikan sejak tahap perancangan sebagai salah satu prinsip dasar keamanan informasi. *Ketiga,* pertahanan siber mengandung unsur kebijakan, kelembagaan, teknologi dan infrastruktur pendukung serta Sumber Daya Manusia. *Keempat,* implementasi pertahanan siber harus dilakukan oleh SDM yang memiliki kompetensi, integritas yang tinggi dan terlindungi. *Kelima,* dilakukan secara efektif dan efisien dalam bentuk keamanan fisik dan keamanan logis secara terintegrasi dengan memanfaatkan semaksimal mungkin teknologi terbuka dan produk Indonesia dalam rangka kemandirian dan kedaulatan. *Keenam,* penetapan zona pengamanan berdasarkan klasifikasi SDM yang terlibat seperti administrator, pengguna dan tipe lain. *Ketujuh,* mengacu kepada prinsip-prinsip tata kelola yang menjamin terwujudnya pengawasan melekat dalam pertahanan siber. *Kedelapan,* menjamin bahwa implementasi sistem siber aman dan tahan terhadap serangan siber lawan. *Kesembilan,* mengembangkan kondisi yang lebih

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 378-382

menguntungkan untuk tindakan ofensif. *Kesepuluh,* menghindari kerugian pada sistem komputer yang tidak diinginkan (Peraturan Menteri No 82 thn 2014).

Sasaran Pertahanan Siber

Sasaran yang hendak dicapai pedoman ini adalah : pertama, terdapatnya pemahaman atas situasi dan kondisi terkini menyangkut ancaman dan serangan siber khususnya dalam sektor pertahanan termasuk penanganannya baik di dalam dan luar negeri. Kedua, Terbangunnya kesadaran (awareness) akan arti penting pertahanan siber dalam rangka pengamanan sumber daya informasi khususnya sektor pertahanan dan secara umum bagi infrastruktur kritis nasional. Ketiga, terlibatnya semua pihak terkait secara penuh dan terpadu dalam inisiatif pertahanan siber di lingkungan Kemhan/TNI. Keempat, terbangunnya potensi sumber daya dalam pengembangan pertahanan siber sebagai bagian dari sistem pertahanan negara. Kelima, terumuskannya strategi penangkalan, penindakan dan pemulihan bidang pertahanan siber. Keenam, tersedianya acuan bagi penyediaan fasilitas, sarana dan prasarana serta pengetahuan dan ketrampilan guna mendukung langkah langkah persiapan, pembangunan, pengembangan dan penerapan pertahanan siber.

Tugas, Peran dan Fungsi Pertahanan Siber

Dalam rangka memastikan pertahanan siber dapat dijalankan secara baik, maka diperlukan dukungan kelembagaan yang kuat, profesional dan andal untuk memastikan tujuan dari pertahanan siber dapat tercapai. Kegiatan pengorganisasian ini diharapkan dapat mewujudkan peran dan fungsi sebagai integrator, inisiator, koordinator dan mediator dari seluruh kegiatan pengamanan informasi di lingkungan Kementerian Pertahanan dan TNI. Tugas pertahanan siber diantaranya, menjamin terwujudnya ketahanan siber di lingkungan Kemhan dan TNI, menjaga sumber daya informasi Kemhan atau TNI agar terlindung dari gangguan dan penyalahgunaan atau pemanfaatan pihak-pihak lain, menjaga keamanan informasi infrastruktur kritis TIK Kemhan atau TNI, mendorong partisipasi aktif pemanfaatan ruang siber yang aman melalui kerjasama kemitraan nasional dan internasional lintas sektoral, membangun kapasitas pertahanan siber berupa kemampuan penangkalan, penindakan dan pemulihan, dan menyelenggarakan dan mengembangkan pengelolaan kelembagaan Pertahanan Siber yang bertanggung jawab, efektif, efisien dan akuntabel.

Peran pertahanan siber diantaranya, sebagai saringan data antara satuan jajaran yang aman untuk menjaga keamanan jaringan strategis antara lembaga dalam upaya menjaga kerahasiaan dan ketersediaan atau keberlangsungan jaringan yang diterapkan secara konsisten pada semua lembaga terkait, sebagai model pusat data dan sarana pendukung yang aman untuk menjaga keamanan informasi strategis yang dapat menjadi contoh/acuan bagi semua lembaga, model pusat data dan sarana pendukung harus memberi acuan yang memperhatikan: (a) Pemanfaatan teknologi tepat guna (usability) (b) Kemampuan pengelolaan dan pengoperasian yang efisien dan mandiri (manageability) (c) Kemampuan pengembangan lebih lanjut (scalability).

Fungsi pertahanan siber diantaranya untuk *Pertama,* menjamin tercapainya sinergi kebijakan pertahanan siber. *Kedua,* membangun organisasi dan tata kelola sistem penanganan keamanan siber. *Ketiga,* membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan siber. *Keempat,* membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber. *Kelima,* mewujudkan kesadaran keamanan siber. *Keenam,* meningkatkan keamanan sistem siber sektor pertahanan. *Ketujuh,* mewujudkan riset dan pengembangan untuk mendukung pembinaan dan pengembangan kemampuan Pertahanan Siber. *Kedelapan,* menyelenggarakan kerjasama nasional dan internasional guna pembinaan dan pengembangan kemampuan pertahanan siber (Peraturan Menteri No 82 thn 2014).

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 378-382

Kesimpulan

Terorisme siber adalah isu strategis yang saat ini perlu menjadi perhatian. Semua lini sektor, baik swasta maupun pemerintah, harus dapat memandang masalah ini secara menyeluruh karena dampak dari masalah ini berkenaan dengan aspekaspek astagatra ketahanan nasional Indonesia.

Dalam rangka persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan atau TNI, diperlukan persamaan pemahaman tentang prinsip-prinsip, sasaran serta tugas, peran dan fungsi pertahanan siber yang akan dilaksanakan. Hal ini menjadi acuan dalam penetapan resiko yang ditimbulkan sehingga menentukan langkah-langkah pertahanan siber yang akan diambil.

Penulisan Daftar Pustaka

Arifin, Zaenal. *"Metode penulisan ilmiah".* Tanggerang, Maret 2017. 41.

Diapoldo, Fujiyama. *"Keamanan Siber".* Semarang, Agustus 2022. 197.

Fitriana, Bambang. *"Jurnal : Cyberterrorism Suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional"*. 2017.

Peraturan menteri pertahanan nomor 82 tahun 2014 tentang pedoman pertahanan siber.

Putri, Okti. *"Skripsi : Tinjauan Yuridis Tindak Pidana Cyber Terrorism Dalam Perspektif Kejahatan Transnasional Terorganisir".* 2020.

Tanzeh, Ahmad. *"Metodologi Penelitian Praktis"*. Yogyakarta, Teras 2011. 83.