Yayan Irfan Ferdiwan
5215100062
KAI-B

Peraturan Menteri Pertahanan Indonesia No 82 Tahun 2004

Tentang Pertahanan Siber(Cyber Crime)

Tujuan

Menjabarkan Pedoman Strategis Pertahanan Nirmiliter perlu ditetapkan Pedoman Pertahanan Siber.

Mengamankan informasi yang ada dalam negara.

Menanggulangi permasalahan yang timbul(hacking, cracking dsb.).

Sebagai referensi utama dalam pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI.

Hal Menarik

Dalam peraturan yang saya temukan ini, berisi data yang sangat banyak. Berisikan 74 halaman mulai dari latar belakang pembuatan, kondisi saat itu, keperluan pertahanan siber, prinsip pertananan, sasaran pertahanan cyber, tugas, peran, fungsi cyber, regulasi/kebijakan, kelembagaan, infrastruktur, sumber daya manusia, tahapan penyelenggaraan pertahanan siber dan pentahapan kegiatan pertahanan siber.

Ringkasan

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) pada saat ini sudah memasuki semua aspek kehidupan masyarakat di dunia. Pemanfaatan TIK tersebut mendorong terbentuknya satu komunitas yang terhubung secara elektronik dalam satu ruang yang sering disebut ruang siber (cyber space). Sistem elektronik termasuk jaringan internet pada saat ini dimanfaatkan untuk mendukung berbagai kegiatan di sektor usaha, perdagangan, layanan kesehatan, komunikasi dan kepemerintahan, serta sektor pertahanan. Semakin meluasnya dan meningkatnya pemanfaatan TIK khususnya melalui jaringan internet diiringi pula dengan meningkatnya aktivitas ancaman. Ancaman itu antara lain upaya membobol kerahasiaan informasi, merusak sistem elektronik dan berbagai perbuatan melawan hukum lainnya.

Dengan memperhatikan hal di atas, ruang siber perlu mendapatkan perlindungan yang layak guna menghindari potensi yang dapat merugikan pribadi, organisasi bahkan negara. Istilah pertahanan siber muncul sebagai upaya untuk melindungi diri dari ancaman dan gangguan tersebut.

Pertahanan siber bertingkat dari lingkup perorangan, kelompok kerja, organisasi sampai dengan skala nasional. Perhatian yang khusus diberikan pada sektor yang mengelola infrastruktur kritis seperti pertahanan keamanan, energi, transportasi, sistem keuangan, dan berbagai layanan publik lainnya. Gangguan pada sistem elektronik pada sektor-sektor ini bisa menyebabkan kerugian ekonomi, turunnya tingkat kepercayaan kepada pemerintah, terganggunya ketertiban

umum dan lain lain. Resiko ini yang menjadi pertimbangan diperlukannya pertahanan siber yang kuat dalam satu negara.

Sebagai instansi pemerintah, Kementerian Pertahanan dan Tentara Nasional Indonesia memiliki dua kepentingan dalam pertahanan siber. Pertama, untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya. Kedua, mendukung koordinasi pengamanan siber di sektorsektor lainnya sesuai kebutuhan. Oleh karenanya Kemhan/TNI perlu mengambil langkah langkah persiapan untuk dapat menjalankan perannya dalam pertahanan siber sebagaimana diuraikan di atas.

Pedoman ini disusun untuk menjadi acuan bagi tahapan persiapan, pembangunan, pelaksanaan dan pemantapan pertahanan siber di lingkungan Kemhan/TNI. Acuan yang disusun meliputi aspek kebijakan, kelembagaan, teknologi/infrastruktur dan sumber daya manusia. Setiap aspek tersebut sama penting dan bersifat saling mendukung sehingga memerlukan perhatian dari semua pihak yang terkait dengan pertahanan siber sesuai dengan peran dan tanggung jawabnya.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara menyebutkan bahwa pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI) dan keselamatan segenap bangsa dari segala bentuk ancaman, baik ancaman militer maupun non-militer. Ancaman nonmiliter khususnya di ruang siber telah menyebabkan kemampuan negara dalam bidang soft dan smart power pertahanan harus ditingkatkan melalui strategi penangkalan, penindakan dan pemulihan pertahanan siber (cyber defense) dalam rangka mendukung penerapan strategi nasional keamanan siber yang dimotori oleh Kementerian Komunikasi dan Informatika.

Di dalam Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa pemanfaatan teknologi informasi membutuhkan pengamanan dalam rangka menjaga kerahasiaan, keutuhan dan

ketersediaan informasi. Dalam Undang-undang tersebut, informasi dalam bentuk elektronik diakui secara hukum dan perbuatan yang terkait dengan sistem elektronik, baik selaku penyelenggara maupun selaku pengguna memiliki pertanggungjawaban hukum yang selanjutnya diatur dalam berbagai peraturan perundangan.

Kementerian Komunikasi dan Informatika RI, selaku leading sector Pemerintah RI dalam bidang Telekomunikasi dan Informatika memiliki 5 agenda kebijakan keamanan siber dalam membangun Secure Cyber Environment, melalui penerapan model strategi “Ends-Ways-Means” yang fokus pada sasaran, prioritas dan aksi yang terukur. Kelima kebijakan tersebut adalah: Capacity Building, Policy and Legal Framework, Organizational Structure, Technical and Operational Measures, dan International Cooperation. Selanjutnya peran Kementerian Komunikasi dan Informatika sebagai pengelola keamanan siber nasional dan kebijakan yang

ditetapkannya dalam peran tersebut akan menjadi acuan utama bagi perumusan pedoman pertahanan siber ini.

Dihadapkan dengan kepentingan nasional, Kementerian Pertahanan RI sangat perlu untuk memahami, mengkaji, mengukur, mengantisipasi dan menyiapkan tindakan yang dibutuhkan. Oleh karena itu Kemhan/TNI perlu menyusun suatu pedoman pertahanan siber sebagai acuan yang digunakan untuk persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI.