OPINI

TRANSFORMASI DIGITAL SEBAGAI PENGUNGKIT KINERJA KEMENTERIAN PERTAHANAN

Evi Savitri, S. Kom., M.A.
Analis Pertahanan Negara Ahli Madya Kemhan RI
Mahasiswa Pasca Sarjana Prodi Doktor Ilmu Pemerintahan IPDN
Dosen: Prof. Dr. Ismail Nurdin, M.Si

Transformasi digital telah menjadi agenda utama di berbagai sektor, termasuk sektor pertahanan. Di era digital saat ini, ancaman keamanan yang dihadapi semakin kompleks dan memerlukan pendekatan holistic. Oleh karena itu, Kementerian Pertahanan telah menerapkan transformasi digital dan sistem informasi terpadu untuk meningkatkan efisiensi, transparansi dan efektivitas operasionalnya. Transformasi Digital di Kementerian Pertahanan menerapkan teknologi digital untuk mentransformasi proses bisnis, meningkatkan efisiensi operasional dan memperkuat kapabilitas pertahanan. Pada Agustus 2020, Presiden Jokowi memaklumatkan transformasi digital Indonesia melalui lima program utama, antara lain perluasan akses dan peningkatan infrastruktur digital, pengembangan peta jalan transformasi digital di sektor-sektor strategis percepatan integrasi pusat data nasional, penyiapan sumber daya manusia talenta digital, dan regulasi terkait pendanaan transformasi digital. https://nasional.kompas.com/read/2021/05/16/15264301/transformasi-digital-pada-sistem-pertahanan-dan-keamanan?page=all#page2

Menurut Eric Schmidt (Schmidt & Cohen, 2015) Transformasi digital adalah proses adopsi teknologi digital untuk mengubah cara organisasi beroperasi dan memberikan nilai tambah. Hal ini sejalan dengan konteks Kementerian Pertahanan, proses administrasi, pengembangan sistem informasi berbasis

teknologi, dan penerapan teknologi canggih seperti big data, cloud computing dan kecerdasan buatan merupakan upaya transformasi digital.

Selain itu transformasi digital di Kementerian Pertahanan juga diterapkan di bidang Intelijen melalui penggunaan data dari medsos, sensor, dan lain-lain yang digunakan untuk menganalisis ancaman dan membuat mitigasi risiko serta penanggulangannya. Di bidang logistik dengan menggunakan data tentang demand, suplai dan Lokasi untuk mengoptimalkan rantai pasokan. Di bidang operasi militer melalui analisis data medan perang yang mendukung pengambilan taktik Keputusan. Di bidang perencanaan strategis guna merumuskan strategi dan kebijakan jangka panjang serta mengukur kinerja organisasi

Penerapan transformasi digital di Kementerian Pertahanan merupakan langkah strategis untuk meningkatkan efisiensi opeasional, transparansi dan efektivitas serta akurasi laporan kinerja. Ketersediaan data yang akurat, relevan dan komprehensif merupakan asset yang sangat penting agar pemimpin dapat mengidentifikasi tren, pola dan peluang dalam pengambilan keputusan yang lebih baik. Data juga dapat mengidentifikasi potensi risiko dan memberikan informasi langkah-langkah mitigasi, sumber daya, efisiensi biaya dan peningkatan produktivitas sehingga pemimpin dapat membuat acuan prediksi yang lebih akurat dan relevan. Untuk itu diperlukan teknologi pendukung pengambilan keputusan berbasis data misalnya *Business Inteligence* yang dapat memvisualisasi berbagai jenis data menjadi informasi yang lebih mudah dipahami. Selain itu penggunaan kecerdasan buatan juga dapat memproses analisis data secara otomatis yang didukung oleh digitalisasi administrasi, pengembangan sistem informasi, *big data* dan *cloud computing*.

Dalam konteks ini, Kementerian Pertahanan melihat transformasi digital sebagai inovasi yang perlu diadopsi untuk meningkatkan efisiensi dan efektifitas operasional. Hal ini didukung oleh teori Difusi Inovasi yang disampaikan oleh Evverest Rogers dalam jurnal yang ditulis oleh (Ummah, 2019). Dalam bukunya yang berjudul *Diffusion of Innovasion (DOI*), Rogers

menyampaikan konsep difusi inovasi yaitu inovasi, difusi dan adopsi. Teori ini menjelaskan bagaimana ide baru melalui tahap adopsi oleh berbagai partisipan dalam memulai penggunaan ide baru tersebut.

Contoh transformasi digital terkini yang telah diterapkan oleh Kementerian Pertahanan adalah inovasi pertahanan siber yang dilaksanakan oleh Pushansiber Bainstrahan Kemhan. Inovasi dan integrasi teknologi diharapkankan dapat meningkatkan kemampuan anlasisi intelijen, mempercepat pengambilan Keputusan dan meningkatkan efisiensi operasional. Penguatan pertahanan siber di Kementerian Pertahanan adalah suatu keharusan mengingat ancaman siber yang semakin terorganisis, canggih dan sulit terdeteksi. Hal ini disebabkan pelaku serangan siber memiliki keahlian di bidang teknologi informasi yang memanfaatkan kerentanan sistem pertahanan modern yang sangat tergantung pada teknologi. Kementerian Pertahanan menyimpan data sensitif yang sangat berharga seperti rencana operasi, intelijen dan informasi tentang personel serta data alutsista.

Namun, dibalik manfaat yang besar, transformasi digital khususnya dalam pertahanan siber juga berakibat munculnya sejumlah tantangan lain dan kontroversi yang kompleks. Kontroversi utama terhadap keamanan data rahasia negara, rencana operasi dan privasi serta informasi intelijen menjadi risiko ancaman serius. Hal ini sebagai akibat dari meningkatnya frekuensi dan kompleksitas serangan siber penyalahgunaan data pribadi yang dapat melumpuhkan infrastruktur kritis. Menurut UU No. 3 Tahun 2002 tentang Pertahanan Negara, ditetapkan bahwa ancaman dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk diantaranya ancaman dan perang siber (*Cyber War*). Perang siber merupakan perang dengan menggunakan jaringan internet atau cyber space yang berupa penyerangan terhadap sistem informasi. Pelaku memanfaatkan teknologi komputer dan internet. Melalui internet pelaku dengan mudah melakukan kejahatan tanpa perlu mengeluarkan banyak biaya dan sumber daya. Paradigma keamanan nasional telah bergeser pada jaminan keamanan pribadi seluruh warga negara dimana kewajiban

pokok dari negara adalah memberikan keamanan terhadap warganya. Berdasarkan laporan semester pertama tahun 2024 hasil analisis AwanPintar.id, total seluruh serangan siber di Indonesia mencapai 2.499.486.085 serangan. Ini berarti bahwa Indonesia rata-rata mengalami 13.733.440 serangan siber per hari.

https://www.awanpintar.id/wpcontent/uploads/2024/08/2024_AwanPntar.id_Laporan_Ancaman_Digital_sem1_2024_Green.pdf

Menyikapi kontroversi diatas, perlu dilakukan pendekatan yang komprehensif dan berimbang dengan beberapa rekomendasi yang dapat dipertimbangkan:

1. Penguatan Sistem Keamanan Siber dengan melakukan pengembangan sistem deteksi intrusi yang terbaru, enkripsi data.
2. Investasi Sumber Daya Manusia melalui Pendidikan dan pelatihan yang berkelanjutan

3. Peningkatan investasi dengan mengalokasikan anggaran yang lebih besar yang dapat digunakan untuk membeli peralatan siber yang canggih, melatih SDM dan melakukan penelitian untuk memperkuat pertahanan siber.
4. Kolaborasi internasional dengan negara-negara lain di dunia dalam hal pengembangan norma dan aturan internasional yang mengatur penggunaan teknologi militer.
5. Meningkatkan Transparansi dan Akuntabilitas dalam pengambilan Keputusan terkait penggunaan teknologi militer dan mekanisme akuntabilitas yang jelas.
6. Kerjasama dengan Perusahaan teknologi dan penyedia layanan keamanan siber dari sektor swasta dapat memberikan akses terhadap teknologi dan keahlian yang dibutuhkan.

Penguatan pertahanan siber di Kementerian Pertahanan melalui transformasi digital merupakan investasi jangka panjang yang sangat dibutuhkan dan penting untuk menjada keamanan serta kedaulatan negara. Melalui pendekatan yang komprehensif dan berkelanjutan, Indonesia dapat membangun dan memiliki pertahanan siber yang kuat dan Tangguh.