

Peran Pelacak *Find My Device* untuk Memperkuat Pertahanan Negara: Materi Pembelajaran pada Pelatihan Keamanan Siber

Charla Susanti¹, R. Okta Kurniawan²

¹Ditjen Pothan Kemhan, shantierna69@gmail.com

²Badiklat Kemhan, cencya95@gmail.com

ABSTRAK

Pelacak *Find My Device* (FMD) merupakan teknologi yang dapat digunakan untuk melacak perangkat elektronik yang hilang atau diretas dan memiliki potensi besar dalam mendukung pertahanan negara. Di bidang pertahanan negara, pemanfaatan sistem pelacakan semacam ini dapat memperkuat keamanan dan infrastruktur siber negara, terutama dalam konteks penguatan keamanan siber dan pengembangan sumber daya manusia siber. Penelitian ini bertujuan untuk mengeksplorasi bagaimana sistem pelacakan seperti FMD dapat dimanfaatkan dalam pengembangan Sumber Daya Manusia Siber, guna mendukung pertahanan negara di era digital yang semakin kompleks. Pengembangan SDM Siber adalah untuk membekali para profesional siber dengan keterampilan praktis dalam memitigasi risiko terkait perangkat yang hilang atau diretas, serta meningkatkan kapabilitas negara dalam melindungi data sensitif dari ancaman perang hibrida. Dengan menggunakan metode penelitian deskriptif-analitis yang berbasis pada studi literatur dan analisis sistem, penelitian ini mengkaji cara teknologi pelacakan dapat membantu identifikasi dan mitigasi ancaman di dunia maya, serta meningkatkan kesiapsiagaan dan ketahanan siber negara. Hasil penelitian menunjukkan bahwa, melalui pelatihan dan penerapan teknologi pelacakan, SDM yang terlibat dalam keamanan siber dapat mengasah keterampilan dalam pengelolaan perangkat dan data untuk memperkuat pertahanan negara. Pemanfaatan teknologi ini juga berpotensi mempercepat respons terhadap insiden siber, memberikan transparansi dalam pengawasan aset, dan memperbaiki koordinasi antar lembaga terkait pertahanan negara. Oleh karena itu, pendidikan dan pelatihan (diklat) SDM dengan menggunakan sistem pelacakan digital menjadi penting untuk meningkatkan efektivitas pertahanan siber nasional.

Kata kunci: pelacak, *find my device*, pertahanan negara, siber, teknologi, pengembangan SDM, analisis sistem, diklat, keamanan siber.

ABSTRACT

Find My Device (FMD) tracker is a technology that can be used to track lost or hacked electronic devices and has great potential in supporting national defense. In the field of national defense, the use of this kind of tracking system can strengthen the country's cyber security and infrastructure, especially in the context of strengthening cyber security and cyber human resource development. This research aims to explore how tracking systems such as FMD can be utilized in developing Cyber Human Resources, to support national defense in an increasingly complex digital era. cyber human resources development is to equip cyber professionals with practical skills in mitigating risks related to lost or hacked devices, as well as increasing the country's capabilities in protecting sensitive data from the threat of hybrid warfare. Using descriptive-analytical research methods based on literature studies and systems analysis, this research examines how tracking technology can help identify and mitigate threats in cyberspace, as well as increase the country's cyber preparedness and resilience. The research results show that, through training and implementing tracking technology, human resources involved in cyber security can hone skills in managing devices and data to strengthen national defense. Utilization of this technology also has the potential to speed up responses to cyber incidents, provide transparency in asset monitoring, and improve coordination between agencies related to national defense. Therefore, human resource education and training using a digital tracking system is important to increase the effectiveness of national cyber defense.

Keywords: tracker, find my device, national defense, cyber, technology, human resources development, systems analysis, training, cybersecurity.

PENDAHULUAN

Keamanan siber bukan sekadar isu teknis, tetapi kini menjadi pertarungan besar bagi pertahanan negara di era digital. Ancaman terhadap data dan sistem informasi kritis semakin nyata, dan jika kita lengah, bisa saja masa depan kita tergadai. Salah satu alat yang dapat menjadi pedang bermata dua adalah fitur pelacak perangkat seperti *Find My Device* (FMD) di Android dan *Find My iPhone* (FMI) di iOS. Seolah-olah, alat yang dimaksud untuk melindungi perangkat pribadi ini memiliki potensi besar dalam memperkuat atau justru mengancam pertahanan negara.

Dikenal luas sebagai alat pribadi untuk melacak ponsel atau laptop yang hilang, FMD ternyata bisa lebih dari itu. Dengan kemampuannya untuk melacak dan menghapus data dari perangkat yang hilang, fitur ini bisa digunakan untuk memantau perangkat pemerintah dan institusi penting. Bahkan, teknologi ini berpotensi mendeteksi ancaman serius terhadap infrastruktur kritis negara, seperti sistem kelistrikan atau transportasi. Tetapi apakah kita siap dengan dampak penggunaan teknologi ini dalam konteks keamanan nasional?

Di satu sisi, FMD bisa menjadi senjata yang sangat efektif untuk melindungi data sensitif dan mencegah serangan siber. Dalam kondisi tertentu, teknologi ini bisa menghapus data secara jarak jauh dan mencegah informasi penting jatuh ke tangan yang salah. Namun, di sisi lain, penggunaan FMD dalam konteks pertahanan negara menimbulkan pertanyaan besar: sejauh mana kita akan mengorbankan privasi demi keamanan? Apakah kita rela kebebasan pribadi dikorbankan demi perlindungan dari ancaman siber?

Jika tidak diatur dengan ketat, teknologi pelacakan seperti FMD dapat disalahgunakan untuk memantau individu tanpa izin atau tanpa dasar hukum yang jelas. Bagaimana jika pemerintah atau pihak berwenang menggunakan fitur ini untuk melacak setiap langkah kita? Potensi penyalahgunaan ini tentu saja menimbulkan ketakutan dan pro-kontra yang tak terhindarkan. Apakah kita siap menghadapi dunia

di mana privasi kita bisa diabaikan demi alasan keamanan?

Sebagai bangsa yang mengutamakan kebebasan, kita harus bijak dalam menyikapi perkembangan teknologi. Penggunaan FMD dan teknologi pelacakan lainnya harus diimbangi dengan regulasi yang jelas dan tegas, agar tidak melanggar hak asasi manusia. Kita perlu memastikan bahwa teknologi ini digunakan dengan tujuan yang benar-benar untuk melindungi negara, bukan malah merampas hak-hak dasar kita sebagai warga negara.

Dalam dunia yang semakin terhubung ini, pengelolaan dan perlindungan data harus menjadi prioritas utama. Namun, kita juga harus sadar bahwa setiap langkah untuk memperkuat pertahanan negara di dunia maya berpotensi membawa risiko terhadap kebebasan kita. Jadi, siapkah kita mengorbankan privasi demi keamanan? Atau akankah kita mempertahankan kebebasan kita, meskipun itu berarti membuka celah bagi ancaman yang lebih besar?

Berdasarkan pertimbangan tersebut, penelitian ini bertujuan untuk memberikan masukan tentang materi diklat keamanan siber yang tepat untuk meningkatkan kompetensi SDM dalam pemanfaatan FMD. Permasalahannya adalah materi apa saja yang perlu diberikan dalam penguatan kompetensi SDM Siber dan seberapa jauh penggunaan FMD dalam keamanan siber.

METODE PENELITIAN

Penelitian ini berfokus pada aspek kebijakan atau implikasi sosial menggunakan pendekatan deskriptif-analitis yaitu studi literatur dan analisis sistem. Studi literatur dengan melakukan peninjauan penelitian, artikel, dan kebijakan yang ada tentang penggunaan teknologi pelacakan dalam konteks keamanan nasional. Hal ini mencakup jenis teknologi pelacakan, dari GPS hingga pelacakan berbasis jaringan, serta aplikasi dalam pertahanan negara. Analisis sistem dengan melakukan analisis terhadap sistem pelacakan perangkat FMD, termasuk kelebihan dan kekurangan perangkat tersebut. Hal ini mencakup analisis teknis tentang keandalan, skalabilitas, dan kerentanan terhadap serangan atau gangguan.

TINJAUAN PUSTAKA

FMD membahas berbagai aspek teknis, fungsional, dan teoritis yang mendasari aplikasi ini, serta teknologi yang digunakan untuk mengembangkan dan mendukungnya. FMD adalah layanan yang dikembangkan oleh Google untuk membantu pengguna melacak perangkat Android mereka yang hilang atau dicuri. Layanan serupa juga ada pada ekosistem Apple dengan *Find My iPhone*. FMD merupakan aplikasi layanan berbasis *cloud* yang memungkinkan pengguna untuk melacak lokasi perangkat mereka secara *real-time*. Layanan ini menggunakan teknologi geolokasi seperti *Global Positioning System* (GPS), Wi-Fi, dan *Bluetooth* untuk menentukan lokasi perangkat dalam jangkauan tertentu, (Kaplan, E. D., & Hegarty, C. (Eds.). 2017). FMD memberikan opsi untuk mengunci perangkat, menghapus data, atau membunyikan suara pada perangkat yang hilang, guna meningkatkan peluang pengguna untuk menemukan perangkat tersebut. Layanan FMD beroperasi dengan memanfaatkan *cloud computing* untuk menyimpan data lokasi perangkat dan memungkinkan sinkronisasi antara perangkat pengguna dengan server *cloud*. (Thomas, E., Zaigham, M., & Ricardo, P. 2013).

Sedangkan dari aspek teknologi, layanan ini adalah bagian dari ekosistem *Internet of Things* (IoT), yang memungkinkan perangkat fisik terhubung dengan internet dan berkomunikasi untuk memberikan data lokasi secara *real-time* (Uckelmann., 2011). Oleh karena itu, enkripsi *end-to-end* digunakan untuk menjaga keamanan data yang dikirimkan melalui server *cloud*. Keamanan dan privasi pengguna menjadi isu penting dalam aplikasi pelacakan perangkat. Google dan perusahaan lain menerapkan kebijakan privasi yang ketat untuk memastikan data pengguna tidak disalahgunakan (Anderson, R. J. 2010). Data yang ditransmisikan dilindungi melalui penggunaan kriptografi merupakan bagian dari teori keamanan siber (William Stallings. 2015).

Aplikasi FMD adalah sebuah layanan yang dikembangkan oleh Google untuk melacak lokasi perangkat, mengunci perangkat, menghapus data atau menyeting pesan dari jarak jauh, semuanya

melalui akun Google yang terhubung (Ros et al., 2020). Meskipun aplikasi ini tidak dirancang secara khusus untuk kepentingan pertahanan negara, teknologi ini dapat berperan dalam konteks pertahanan dan keamanan, baik dalam penggunaan pribadi maupun oleh militer atau lembaga keamanan negara.

Penggunaan dalam konteks pertahanan negara, aplikasi FMD dapat digunakan untuk melacak lokasi. Meskipun aplikasi ini hanya dapat digunakan untuk perangkat Android, dalam konteks yang lebih besar, aplikasi lain yang serupa untuk perangkat lain juga dapat digunakan dengan tujuan yang sama. Dalam operasi militer atau pengawasan, personel dapat menggunakan perangkat telepon seluler yang dilengkapi dengan aplikasi pelacakan ini untuk memastikan bahwa perangkat mereka tidak jatuh ke pihak yang tidak berwenang, serta untuk memantau lokasi mereka jika terjadi kejadian darurat.

Aplikasi FMD lebih sering digunakan dalam konteks individu atau perusahaan untuk melindungi perangkat pribadi atau perusahaan, dalam ranah pertahanan negara, teknologi serupa mungkin digunakan dalam sistem pelacakan atau pengawasan yang lebih canggih (Babu et al., 2021). Lembaga pertahanan negara, termasuk militer, sering kali mengembangkan sistem pelacakan khusus yang jauh lebih kuat dan aman, yang dirancang untuk melacak perangkat dan personel dalam operasi yang lebih besar. Secara keamanan, aplikasi FMD tidak dirancang dengan tingkat keamanan yang dibutuhkan oleh militer atau badan intelijen untuk melindungi informasi sensitif.

Aplikasi FMD dapat menjadi alat yang efektif untuk menjaga keamanan perangkat, mencegah potensi ancaman, melindungi data sensitif (Ajiga et al., 2024). Namun, penggunaannya harus diatur dengan bijak dan memenuhi regulasi yang berlaku. Pengelolaan terhadap teknologi ini akan mendukung ketahanan dan keamanan negara secara keseluruhan.

Tantangan dan pertimbangan dalam penerapan teknologi pelacakan untuk pertahanan negara yaitu:

1. Penerapan pelacakan perangkat perlu mempertimbangkan aspek privasi dan

perlindungan data. sistem pelacakan harus dirancang untuk memastikan bahwa data yang dikumpulkan hanya digunakan untuk tujuan yang sah dan sesuai dengan peraturan yang berlaku.

2. SDM yang terlatih dalam teknologi pelacakan dan pengelolaan data perlu memiliki keterampilan yang mumpuni untuk menangani sistem yang kompleks dan memiliki tingkat keandalan tinggi. SDM tersebut harus dilatih dalam cara menggunakan, mengkonfigurasi, serta mengamankan perangkat dan sistem pelacakan.
3. Memerlukan koordinasi yang kuat antara berbagai lembaga, seperti militer, kepolisian, dan badan keamanan siber. Dalam hal ini, teknologi pelacakan dapat membantu mempercepat respons terhadap ancaman, namun membutuhkan integrasi sistem yang baik antar lembaga tersebut.
4. Teknologi pelacakan perangkat di sektor pertahanan harus diimbangi dengan pengawasan yang ketat serta pemahaman tentang batasan-batasan hukum terkait penggunaan teknologi ini. Pemerintah perlu memastikan bahwa ada regulasi yang jelas untuk menghindari penyalahgunaan teknologi tersebut.

HASIL DAN PEMBAHASAN

Pelacakan perangkat, seperti FMD, memiliki peran yang signifikan dalam pertahanan negara, terutama dalam konteks perang hibrida. Meskipun tidak langsung berhubungan dengan peperangan konvensional, perang hibrida menggabungkan berbagai taktik, termasuk perang siber, disinformasi, dan aksi non-konvensional, yang sering kali mengancam stabilitas nasional. Dalam situasi ini, teknologi pelacakan perangkat menjadi alat penting dalam menjaga keamanan siber dan melindungi data sensitif.

Pelacakan perangkat memungkinkan intelijen dan aparat keamanan untuk memantau

perangkat yang terlibat dalam kegiatan mencurigakan, baik itu yang digunakan oleh kelompok musuh maupun individu yang terlibat dalam kejahatan terorganisir. Selain itu, FMD juga berfungsi dalam mengidentifikasi sumber serangan siber yang dapat merusak infrastruktur kritis atau mencuri data penting. Dalam hal kebocoran data, teknologi ini dapat membantu dalam pemulihan dan penelusuran jejak serangan siber.

Di ranah sosial dan politik, perang hibrida juga mencakup penyebaran disinformasi dan propaganda untuk memanipulasi opini publik. Dalam konteks ini, FMD dapat membantu mengidentifikasi individu atau kelompok yang terlibat dalam aktivitas subversif, memungkinkan pihak berwenang untuk mengintervensi sebelum kerusakan lebih lanjut terjadi. Selain itu, perangkat ini dapat digunakan untuk mengawasi koordinasi antara kelompok yang mencoba mendiskreditkan pemerintah atau merusak stabilitas negara.

Dalam dunia yang semakin terhubung secara digital, perangkat pemerintah rentan terhadap serangan. Penggunaan teknologi pelacakan memungkinkan otoritas untuk melindungi perangkat tersebut, mencegah kebocoran informasi, dan memastikan bahwa data sensitif tetap aman, terutama di zona konflik. Pelacakan juga membantu dalam memulihkan perangkat yang hilang, yang mungkin berisi informasi penting bagi keamanan nasional.

Namun, penggunaan teknologi pelacakan perangkat dalam pertahanan negara harus diimbangi dengan perhatian terhadap masalah etika dan privasi. Penggunaan teknologi ini harus mengikuti regulasi yang ketat, memastikan bahwa hak privasi individu tetap dihormati. Oleh karena itu, penting untuk memastikan bahwa pelacakan dilakukan dengan batasan hukum yang jelas dan pengawasan yang memadai untuk mencegah penyalahgunaan.

Pengembangan Sumber Daya Manusia (SDM) di bidang siber menjadi elemen penting dalam menjaga pertahanan negara. SDM ini harus terampil dalam mengoperasikan dan mengamankan perangkat pelacakan, serta memahami berbagai tantangan dan potensi yang terkait dengan teknologi ini. Pelatihan dan

pendidikan yang baik dalam hal etika, kebijakan, dan legalitas penggunaan teknologi pelacakan sangat diperlukan untuk mendukung sistem pertahanan yang efektif dan terpercaya.

Secara keseluruhan, meskipun pelacakan perangkat memiliki manfaat yang besar untuk keamanan negara, penggunaannya harus dilakukan dengan hati-hati, selalu mempertimbangkan aspek etika, privasi, dan kepatuhan pada regulasi yang berlaku.

Pelacakan perangkat untuk pertahanan negara dalam Pendidikan dan pelatihan (diklat) siber umumnya memiliki beberapa tujuan utama, antara lain:

- menguji ketahanan sistem pertahanan siber terhadap serangan dunia maya.
- mengajarkan peserta pelatihan keamanan siber bagaimana perangkat dan sistem pelacakan dapat digunakan untuk mengidentifikasi potensi ancaman atau serangan terhadap sistem pertahanan.
- menggunakan pelacakan perangkat sebagai alat untuk pemantauan dan identifikasi ancaman potensial dalam skenario perang siber atau konflik.

Penggunaan pelacakan perangkat dalam diklat siber harus dilakukan dengan mematuhi prinsip-prinsip etika yang ketat. Hal ini termasuk:

- menggunakan teknologi pelacakan hanya pada perangkat yang sah, dan dengan izin yang sesuai.
- keamanan data: Semua data yang dikumpulkan melalui pelacakan perangkat harus diamankan dan tidak disalahgunakan.
- para peserta diklat siber harus diberi informasi yang jelas mengenai penggunaan teknologi pelacakan, termasuk hak privasi mereka.

Penggunaan teknologi pelacakan untuk tujuan pertahanan negara menghadirkan sejumlah risiko, di antaranya:

- teknologi pelacakan dapat memberikan informasi yang tidak akurat atau gagal

berfungsi, yang bisa mempengaruhi hasil latihan atau simulasi.

- pelacakan perangkat dapat membuka celah keamanan, yang jika tidak ditangani dengan baik dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.
- penggunaan pelacakan perangkat harus dikelola dengan hati-hati agar tidak disalahgunakan untuk tujuan yang tidak sah.

Pelatihan keamanan siber memberikan kompetensi peserta didik untuk melindungi perangkat, jaringan, program, dan data dari serangan digital. Dalam pelatihan ini, penggunaan pelacakan perangkat dapat berfungsi untuk:

- Simulasi serangan dunia maya: misalnya, para peserta didik bisa diajarkan bagaimana perangkat mereka bisa dilacak oleh pihak lawan dalam sebuah simulasi serangan.
- Pengelolaan insiden siber: mengajarkan teknik mitigasi jika perangkat atau data dicuri atau dibajak dalam konteks ancaman siber.
- Peningkatan keterampilan deteksi dan respons: melatih peserta didik untuk mendeteksi dan merespons perangkat yang terinfeksi atau dicuri, serta langkah-langkah pemulihan yang diperlukan.

Melalui pelatihan yang melibatkan penggunaan alat pelacak FMD, peserta didik atau personel pertahanan negara dapat lebih memahami pentingnya perlindungan terhadap perangkat mereka, serta tanggung jawab dalam menjaga kerahasiaan data pribadi dan atau negara.

Untuk menguasai penggunaan FMD dalam pertahanan negara, dibutuhkan dua kelompok keterampilan utama. Keterampilan teknis mencakup pemahaman mendalam tentang teknologi FMD, penguasaan sistem operasi Android dan iOS, kemampuan konfigurasi dan penggunaan FMD, serta pemahaman protokol keamanan siber. Selain itu, pengetahuan tentang teknologi GPS dan pelacakan lokasi, serta keterampilan analisis dan penanganan insiden keamanan juga sangat penting.

Sementara itu, keterampilan non-teknis juga memainkan peran krusial. Kemampuan untuk berkomunikasi secara efektif, bekerja sama dalam tim, serta menganalisis dan memecahkan masalah dengan cepat sangat diperlukan. Selain itu, pengambilan keputusan yang tepat dan pemahaman tentang kebijakan serta regulasi terkait pertahanan negara juga menjadi aspek penting dalam menjalankan peran ini.

Beberapa perangkat pelacakan yang sering digunakan di luar konteks militer atau pertahanan negara, tetapi bisa diadaptasi dalam pelatihan keamanan siber antara lain:

- *Find My Device* (Android): Untuk melacak perangkat yang hilang atau dicuri, dapat digunakan untuk mengajari peserta didik bagaimana perangkat mereka bisa dilacak oleh pihak ketiga.
- *Find My iPhone* (Apple): Sama dengan Android, untuk melacak perangkat Apple.
- Pelacakan berbasis GPS dan jaringan: menggunakan teknologi GPS atau triangulasi jaringan untuk melacak perangkat, bisa digunakan dalam latihan untuk menunjukkan seberapa efektif pelacakan dalam situasi tertentu.

Prinsip-prinsip aplikasi FMD dalam konteks pertahanan negara dapat dilihat dari beberapa sudut pandang berikut:

1. Keamanan Nasional.

Aplikasi pelacakan perangkat dapat digunakan untuk menjaga keamanan individu dan negara. Dalam konteks pertahanan negara, teknologi ini bisa membantu untuk melindungi infrastruktur penting. Jika perangkat yang digunakan oleh aparat militer atau pejabat negara hilang atau dicuri, aplikasi ini dapat membantu melacaknya dan mencegah informasi sensitif jatuh ke tangan yang salah. Dan untuk mencegah kejahatan seperti pencurian data atau spionase yang dapat merugikan negara. Melalui pelacakan perangkat yang hilang, data yang ada di perangkat tersebut bisa segera diamankan.

2. Keamanan Data dan Informasi

Dalam dunia yang semakin terhubung secara digital, perangkat pribadi seringkali menyimpan informasi yang sangat penting. Dari sudut pandang pertahanan negara, ada beberapa hal yang perlu diperhatikan:

- **Keamanan Privasi:** Pemerintah perlu memastikan bahwa penggunaan aplikasi pelacakan perangkat tidak mengganggu hak privasi individu atau menciptakan celah untuk penyalahgunaan informasi. Perlindungan data dan hak asasi manusia menjadi penting agar teknologi ini tidak disalahgunakan untuk tujuan pengawasan yang berlebihan.
- **Perlindungan Data Sensitif:** Aplikasi ini dapat membantu dalam melacak perangkat yang mungkin menyimpan informasi yang berkaitan dengan keamanan nasional. Dengan mengamankan perangkat yang hilang, data sensitif terkait pertahanan atau intelijen bisa dijaga.

3. Kesiapsiagaan dan Respons Cepat

Dalam situasi darurat, aplikasi FMD dapat meningkatkan kesiapsiagaan dan respons cepat terhadap ancaman yang mungkin timbul. Sebagai contoh:

- **Pencurian Perangkat Militer atau Pemerintahan:** Jika perangkat yang berisi data strategis atau sensitif jatuh ke tangan yang salah, aplikasi pelacakan dapat membantu dalam menemukan dan mengamankan perangkat tersebut sebelum data lebih lanjut disalahgunakan.
- **Mengurangi Ancaman Terhadap Keamanan Negara:** Aplikasi pelacakan dapat mengurangi potensi ancaman dari kehilangan perangkat yang digunakan dalam operasi keamanan atau pertahanan.

4. Penguatan Sistem Keamanan Siber.
Salah satu elemen penting dalam pertahanan negara adalah sistem pertahanan siber. Aplikasi pelacakan perangkat bisa menjadi bagian dari strategi pertahanan siber yang lebih besar dengan memberikan cara untuk:

- Mengatasi ancaman keamanan siber, jika perangkat yang hilang berisi perangkat lunak yang digunakan dalam operasi pertahanan atau intelijen, pelacakan dapat membantu melacak dan menghentikan perangkat tersebut sebelum data sensitif dapat dibocorkan atau digunakan untuk serangan siber.
- Aplikasi ini dapat membantu mendeteksi pelanggaran keamanan lebih awal, dengan memberi peringatan jika perangkat ditemukan berada di lokasi yang tidak semestinya.

5. Kepatuhan terhadap Hukum
Terkait dengan prinsip pertahanan negara, penggunaan aplikasi pelacakan perangkat harus selalu berada dalam peraturan yang berlaku. Hal ini meliputi:

- Negara harus memastikan bahwa aplikasi pelacakan perangkat ini mematuhi peraturan perlindungan data pribadi dan kebebasan sipil, serta tidak disalahgunakan untuk tujuan pengawasan yang tidak sah.
- Negara harus memastikan bahwa penggunaan teknologi ini dilakukan dengan pengawasan yang tepat dan terbatas, serta hanya digunakan dalam situasi yang benar-benar diperlukan untuk menjaga keamanan negara.

6. Kebijakan dan Strategi Nasional
Penggunaan aplikasi pelacakan perangkat dalam pertahanan negara perlu dimasukkan dalam kebijakan dan strategi nasional yang lebih luas, yang mencakup:

- Pendidikan dan Pelatihan: Aparat negara, terutama yang terlibat dalam pertahanan dan keamanan, harus diberikan pendidikan mengenai penggunaan teknologi ini untuk tujuan yang sah dan strategis.
- Kolaborasi Internasional: Negara perlu menjalin kerjasama internasional untuk menangani ancaman siber yang melibatkan perangkat yang hilang atau dicuri, serta memastikan bahwa standar internasional dalam perlindungan data dipatuhi.

Meskipun FMD sangat berguna, ada beberapa tantangan yang harus diperhatikan terkait pertahanan negara. Keamanan fitur FMD dapat dieksploitasi oleh pihak ketiga bila tidak diterapkan dengan sistem keamanan yang memadai. Oleh karena itu, pelatihan keamanan siber harus mencakup cara melindungi akun yang digunakan. Dan pelacak perangkat membutuhkan akses internet.

FMD efektif dengan menerapkan strategi melalui integrasi dengan sistem keamanan yang lebih besar, sistem manajemen perangkat negara, untuk meningkatkan pengawasan dan respon terhadap ancaman. Strategi kedua, penggunaan FMD untuk personel yang memiliki akses ke data sensitif harus dibekali dengan pelatihan keamanan siber dalam penggunaan teknologi pelacakan perangkat. Untuk memastikan bahwa perangkat yang digunakan dalam tugas negara aman, perlu dilakukan audit dan pengawasan berkala.

Peningkatan kualitas personel dalam penggunaan FMD dapat dilakukan dengan modul pembelajaran FMD pada pelatihan keamanan siber. Mata pelatihan dan materi pembelajaran dapat dilihat pada Tabel 1.

Tabel.1. Modul pembelajaran *Find My Device* pada pelatihan keamanan siber.
Sumber: Materi Training CSCU-Kepemimpinan Perangkat Mobile (2023)

Modul Pembelajaran <i>Find My Device</i>		
Modul	Mata Pelatihan	Materi Pembelajaran
1	Pengenalan FMD dan keamanan siber	1. Pengenalan teknologi FMD 2. Konsep keamanan siber dan pertahanan negara 3. Ancaman keamanan siber dan dampaknya pada pertahanan negara 4. Peran FMD dalam memperkuat pertahanan negara.
2	Konfigurasi dan penggunaan FMD	1. Konfigurasi FMD pada perangkat Android dan iOS. 2. Penggunaan FMD untuk melacak lokasi perangkat. 3. Penggunaan FMD untuk menghapus data perangkat. 4. Penggunaan FMD untuk mengaktifkan mode “Lost Mode”.
3	Keamanan Data dan Informasi	1. Pengamanan data pada perangkat mobile. 2. Enkripsi data dan penggunaan VPN. 3. Pengamanan informasi sensitive. 4. Penggunaan FMD untuk melindungi data perangkat.
4	Analisis Resiko dan Penanganan Insiden	1. Analisis risiko keamanan siber. 2. Penanganan insiden keamanan siber. 3. Penggunaan FMD untuk mendeteksi dan mencegah serangan siber. 4. Penggunaan FMD untuk memantau aktivitas perangkat.
5	Strategi Pertahanan Siber Nasional	1. Strategi pertahanan siber nasional. 2. Peran FMD dalam strategi pertahanan siber nasional. 3. Kerjasama antar Lembaga pertahanan siber. 4. Pengembangan kemampuan siber nasional.
6	Kasus dan Simulasi	1. Studi kasus penggunaan FMD dalam pertahanan negara. 2. Simulasi serangan siber dan penggunaan FMD 3. Analisis kasus dan diskusi. 4. Pengembangan rencana kontijensi.
7	Pengembangan Kemampuan SDM Siber	1. Pengembangan kemampuan SDM Siber. 2. Pelatihan dan sertifikasi keamanan siber. 3. Pengembangan tim keamanan siber. 4. Pengembangan budaya keamanan siber.

KESIMPULAN

Teknologi pelacakan perangkat seperti FMD memiliki potensi besar untuk memperkuat pertahanan negara. Teknologi ini dapat digunakan untuk mengamankan data sensitif, meningkatkan koordinasi antar kementerian/lembaga, memperkuat pengawasan infrastruktur kritis, dan mendukung operasi intelijen. Namun, penerapannya harus dilakukan dengan hati-hati, memperhatikan regulasi yang ada, dan menjaga keseimbangan antara keamanan negara dan hak individu. Pengelolaan yang bijak akan memperkuat ketahanan dan keamanan negara secara keseluruhan.

FMD bekerja dengan menggabungkan berbagai teknologi, seperti GPS, Wi-Fi, Bluetooth, dan jaringan seluler, untuk melacak perangkat yang hilang atau dicuri. Meskipun efektif, sistem ini memiliki keterbatasan yang tergantung pada faktor teknis dan kondisi perangkat. Aspek privasi dan keamanan pengguna juga harus menjadi perhatian utama untuk mencegah potensi penyalahgunaan.

Sebagai bagian dari ekosistem digital, FMD memanfaatkan teknologi geolokasi, cloud computing, dan jaringan seluler untuk membantu melacak perangkat hilang. Dengan terus berkembangnya teknologi, aplikasi ini akan semakin canggih dan dapat mengatasi tantangan akurasi dan konektivitas yang ada.

Meskipun FMD bukan alat yang dirancang khusus untuk peperangan, teknologi ini memiliki peran penting dalam pertahanan negara, terutama dalam konteks perang hibrida. Dengan kemampuannya untuk melacak perangkat yang terlibat dalam kegiatan intelijen, serangan siber, atau penyebaran disinformasi, negara dapat merespons ancaman lebih cepat dan memperkuat keamanan nasional.

Untuk memaksimalkan manfaatnya, penerapan FMD dalam pertahanan negara memerlukan SDM yang terlatih dan sistem yang dapat diandalkan. Pendidikan dan pelatihan dalam bidang siber harus mencakup pemahaman mendalam tentang aspek teknis dan hukum penggunaan teknologi ini, agar infrastruktur dan data negara terlindungi dengan baik. Selain itu, kesadaran akan pentingnya melindungi perangkat digital dalam menjalankan tugas negara juga harus ditingkatkan di kalangan personel negara.

Dengan strategi yang tepat, FMD dapat menjadi elemen kunci dalam memperkuat pertahanan negara.

DAFTAR PUSTAKA

- Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). 1. *Designing Cybersecurity Measures for Enterprise Software Applications to Protect Data Integrity*.
<https://doi.org/10.51594/csitrj.v5i8.1451>
- Anderson, R. J. (2010). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.
- Babu, M. S., Raj, K. B., & Devi, D. A. (2021). *Data security and sensitive data protection using privacy by design technique*. In *2nd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing: BDCC 2019* (pp. 177-189). Springer International Publishing.
- Cryptography, W. S. P. K., & Al Zoubi, R. D. S. *Cryptography And Network Security By William Stallings 3rd Edition Ppt*.
- Hakim, Ihsan. (2024) Penerapan Aplikasi Google Find My Device untuk Pengamanan Perangkat Mobile Android.
<https://doi.org/10.13140/RG.2.2.34014.24648>
https://www.researchgate.net/publication/383039053_penerapan_aplikasi_google_find_my_device_untuk_pengamanan_perangkat_mobile_android
- Kaplan, E. D., & Hegarty, C. (Eds.). (2017). *Understanding GPS/GNSS: principles and applications*. Artech house.
- Kennedy, M. (2002). *The global positioning system and GIS*. CRC Press.
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. LN. 2019/No. 185, TLN No. 6400, jdih.setneg.go.id
- Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan

- Manajemen Krisis Siber. LN 2023/No. 99, jdih.setneg.go.id
- Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. BN. 2014/No. 1712, peraturan.go.id.
- Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintah Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintah berbasis Elektronik. BN. 2021/No. 541, jdih.bssn.go.id
- Purbo, O. W. (2020). Mid 2020 Cyber Security Threat, Tips dan Proposal Strategi Mitigasi Nasional.
- Ros, D., Thomson, G., & Taylor, R. G. (2020). *Remote device management*.
- Sari, Rita Puspita. (2024). 6 Cara Efektif Melindungi Privasi dan Keamanan Data di Smartphone. <https://digitalcitizenship.id/tips-trik/keamanan-data-di-smartphone>
- Suud, Yuswardi A., (2020). Pelacakan Data Lokasi Ponsel oleh Pemerintah, Haruskah Kita Khawatir? [https://www.cyberthreat.id/read/9394/Pela](https://www.cyberthreat.id/read/9394/Pelacakan-Data-Lokasi-Ponsel-oleh-Pemerintah-Haruskah-Kita-Khawatir)
- cakan-Data-Lokasi-Ponsel-oleh-Pemerintah-Haruskah-Kita-Khawatir
- Thomas, E., Zaigham, M., & Ricardo, P. (2013). *Cloud computing concepts, technology & architecture*.
- Uckelmann, D., Harrison, M., & Michahelles, F. (Eds.). (2011). *Architecting the internet of things*. Springer Science & Business Media..
- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. LN. 2008/No. 58, TLN No. 4843, LL Setneg.
- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. LN. 2022/No. 196, TLN No. 6820, jdih.setneg.go.id.
- Undang-Undang Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara. LN.2019/No. 211, TLN No. 6413. peraturan.go.id.
- Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara. LN. 2002/No. 3, TLN No. 4169, LL Setneg.
- Wamala, Frederick. (2011). *The ITU National Cybersecurity Strategi Guide. International Telecommunication Union*.