FisiPublik: Jurnal Ilmu Sosial dan Politik
https://journal.uwgm.ac.id/index.php/fisipublik
P-ISSN: 2528-2689; E-ISSN: 2540-9751
November 2024, Vol.9 No. 2

CYBER SECURITY AWARENESS DALAM PENGGUNAAN GEO- TAGGING DI MEDIA BARU DAN POTENSI IMPLIKASINYA TERHADAP KEAMANAN NASIONAL

Adji Yuwana Pratama[1], Ridwan[2],
Adji Yuwana Pratama, Universitas Pembangunan Nasional Veteran Jakarta[1]
Ridwan, Universitas Pembangunan Nasional Veteran Jakarta [2]
2410426007@mahasiswa.upnvj.ac.id, ridwan.fisip@upnvj.ac.id, 081298828784,
Correspondence Email: 2410426007@mahasiswa.upnvj.ac.id

Abstract

This article on cyber security awareness in the use of geo-location in New media and its potential implications for national security explains the phenomenon of digital activities that are considered to endanger national security. The activities in question include geo-location tagging, video and photo recording in vital state objects, especially the TNI headquarters. This research uses a qualitative method with a descriptive approach with literature study data retrieval techniques In this research the author uses a cyberpolitics perspective The results of the analysis in this study are the lack of understanding of cyber threats and attacks from state apparatus and civilians. Therefore, the author suggests that the government make regulations governing how to move in vital objects owned by the state, especially the TNI and Polri, the need for socialization to the apparatus and civilians regarding the importance of Cyber Security Awareness and cyber security systems that are relevant to the latest potential threats.

Keywords*: Cyber Security Awareness; Geo tagging, New Media*

Abstrak

Artikel kesadaran keamanan siber dalam penggunaan geo-lokasi di media Baru dan potensi implikasinya terhadap keamanan nasional ini menjelaskan fenomena aktivitas digital yang dianggap dapat membahayakan keamanan nasional. Aktivitas yang dimaksud misalnya melakukan penandaan geo lokasi, perekaman video dan foto di objek-obek vital negara khususnya markas TNI. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif dengan teknik pengambilan data studi kepustakaan Dalam penelitian ini penulis menggunakan perspektif *cyberpolitics* Hasil analisa dalam penelitian ini yaitu kurangnya pemahaman mengenai ancaman dan serangan siber dari aparatut negara dan warga sipil. Oleh karena itu penulis menyarankan agar pemerintah membuat regulasi yang mengatur bagaimana beraktivitas di objek vital milik negara khususnya TNI dan Polri, perlunya sosialisasi kepada aparatur dan warga sipil mengenai pentingnya Cyber Security Awareness dan sistem keamanan siber yang relevan dengan potensi ancaman terkini

Kata kunci: Kesadaran Keamanan Siber; Penandaan Geografis, Media Baru

Received	**:**	18 November 2024
Accepted	:	27 November 2024

Published	:	30 November 2024
Copyright Notice	:	**Authors retain copyright and grant the journal right of first publication** with the work simultaneously licensed under a **Creative Commons Attribution 4.0 International License** that allows others to share the work with an acknowledgement of the work's authorship and initial publication in this journal. 

1. LATAR BELAKANG

Dunia digital mengalami perkembangan yang signifikan, tentunya hal ini berdampak pada kehidupan bernegara, tak terkecuali pada bidang politik. Relevansi digital dan politik meliputi beberapa aspek yang di naungi dalam kajian *cyberpolitics*. Nazli berpendapat kajian *cyberpolitics* meliputi konteks keamanan internasional, kebijakan, dan interaksi antara negara serta aktor non-negara di ruang digital (Choucri, 2012). Berbagai fenomena politik yang terjadi dalam beberapa dekade ini tidak lepas dari aktivitas cyberpolitics. Case arab Spring pada tahun 2011, disusul fenomena serangan Ransomware yang menyerang 99 negara pada 2017 (BBCnews, 2017), serangan peluru kendali dalam konflik di Timur Tengah, serangan bom pager di Lebanon pada 2024 semakin menguatkan peran cyberpolitics dalam dunia politik.

Berdasarkan 3 (tiga) case di atas, differensiasi atas aktor, bentuk dan impact dari *cyberpolitics* semakin bervariasi. Hal ini sangat berpotensi untuk menimbulkan kerugian materil, korban jiwa hingga kedaulatan sebuah negara semakin besar. Melihat fenomena serangan peluru kendali di Timur Tengah, penulis menilai pentingnya untuk mengkaji lebih dalam mengenai keamanan objek-objek startegis di Indonesia dari sudut pandang cyber politics. Selain ketiga teknologi di atas juga berpotensi menimbulkan potensi keamanan dalam kegiatan spionase (mata-mata) misalnya penggunaan drone otomatis untuk pemantauan ke object-object vital berbentuk fisik milik negara seperti markas dan pangkalan militer, istana kepresidenan, laboratorium yang berhubungan dengan sistem pertahanan negara.

Dalam literatur review dari Arip Nurahman dan Pandu Pribadi (2023) mengenai Rudal Canggih dari tiga negara superpower. Dalam beroperasi, Sistem peluru kendali menggunakan bebearpa teknologi siber yang canggih seperti (Nurahman & Pribadi, 2023). Global Positioning System (GPS) berfungsi untul meningkatkan ketepatan dalam membaca posisi dari sebuah target (Din, dkk., 2015). Teknologi sensor untuk mendeteksi sasaran dengan cepat dan akurat. GPS juga memliki fungsi untuk mendeteksi sasaran yang tidak statis dan menyediakan informasi yang lebih komprehensif mengenai dimensi, rupa, dan tipe (Xu et, al., 2019). Teknologi kontrol, Sistem GPS dapat mengatur kecepatan, arah, dan lokasi peluru kendali saat di udara (Sarfaraz et al., 2015). Menurut Waskito, dkk. Untuk dapat menemukan lokasi object vital secara akurat teknologi. Teknologi *Global Positioning System* (GPS) menggunakan teknologi AVL (*Automated Vehicle Locater*) untuk menentukan lokasi kordinat object yang akan menjadi sasaran (Waskito, Nachrowie, & Suprayogi, 2017). Saat ini hampir smeua alat telekomunikasi genggammenggunakan teknologi GPS, selain itu beberapa aplikasi yang ada di

Handpone juga menggunakan teknologi GPS sebagai feature, contohnya Google Maps, Whatsapp, Insragram, Facebook. Beberapa aplikasi tersebut merupakan aplikasi yang sering digunakan oleh masyarakat umumnya dan aparatur negara pada khususnya untuk keperluan sehari-hari. Penggunaaan aplikasi berbasis GPS tersebut menurut penulis bisa membahayakan pertahanan negara, khususnya terkait kerahasiaan keberadaan obejk-objek vital milik negara. Hal ini dikarenakan teknologi GPS saat ini bisa menghasilkan output data berupa kordinat lokasi, foto, video, audio dan catatan. Oleh karena itu sangat penting bagi masyarakat dan aparat pemerintahan untuk dapat mengetahui, memahami dan menjalankan *Cyber Security Awarenesss* dalam menggunakan berbagai aplikasi dan teknologi canggih.

Berdasarkan data yang penulis dapatkan dari hasil penelusuran melalui google maps, dengan menggunakan kata kunci TNI AD (terdapat > 10 lokasi yang berhubungan dengan kata kunci terbut di wilayah Jabodetabek. Dimana jika link tersebut di klik maka akan dapat muncul berbagai informasi seperti: alamat, nomor telepon, website, jam operasional, foto, video, notes, koordinat, review, share, copy, save lokasi, lokasi lain terdekat. Sedangkan berdasarkan pencarian melalui social media instagram dengan menggunakan kata kunci TNI AD terdapat (lebih dari) > 10 lokasi di wilayah Jabodetabek. Adapun jika salah satu item lokasi di klik akan muncul beberapa feature seperti detail alamat, foto dan video, laporkan, link ke Google Maps, copy link, save loaksi, QR dan share

Dua contoh di atas menunjukkan bahwa object-object vital militer di Indonesia sangat mudah diacces baik oleh masyarakat maupun oleh pihak asing. Berdasarkan Undang-Undang Republik Indonesia nomor 5 Tahun 2018 yang dimaksud objek vital Strategis adalah kawasan, tempat, lokasi, bangunan, atau instalasi yang (1) Menyangkut hajat hidup orang banyak, harkat dan martabat bangsa. (2) Merupakan sumber pendapatan negara yang mempunyai nilai politik, ekonomi, sosial, dan budaya; atau (3) Menyangkut pertahanan dan keamanan yang sangat tinggi (Kementerian Pertahanan Republik Indonesia, 2018). Mudahnya seseorang untuk memasukkan, mengajukan perubahan Geo tagging di berbagai aplikasi yang dapat menampilkan lokasi dan data lainnya terhadap object vital negara perlu diiringi dengan pengetahuan dan pemahaman mengenai *Cyber Security Awareness* baik masyarakat secara individu, aparatur negara secara personal maupun kelembagaan.

Berdasarkan berbagai tantangan yang dihadapi *cyberpolitics* sebagaimana dijabarkan di atas, maka dalam penelitian ini penulis akan fokus pada kajian *cyberpolitics* mengenai pentingnya *Cyber Security Awareness* dalam melakukan aktivitas digital Geo Tagging di soaial media dan google maps dan potensi dampaknya terhadap keamanan nasional. Untuk

memperluas khasanah penelitian ini, penulis akan melakukan elaborasi ke beberapa penelitian sudah dilakukan oleh peneliti lain dengan topik yang memiliki relevansi dengan penelitian ini. Beberapa penelitian yang sebelumnya sudah dilakukan diantaranya dari Edy Soesanto, dkk. Menyatakan bahwa potensi ancaman *cybercrime* yang ada di Indonesia antara lain *hacking, cracking, cyber sabotage,* dan *spyware* Oleh karena itu diperlukan managemen resiko dan ahli untuk mengembangkan pusat keamanan siber untuk mengamankan objek-objek vital (Soesanto dkk., 2023).

Dalam penelitian yang dilakukan Valli dan Hannay menyatakan bahwa geo tagging banyak digunakan dalam berbagai media sosial. Penggunaan GeoTagging dapat digunakan untuk untuk menindaklanjuti kejahatan dan mengurangi beban kerja dalam mengumpulkan intelijen dan menemukan TKP (Valli and Hannay, 2010). Sementara Sutrisno dalam penelitiannya yang berjudul tantangan menjaga personal security prajurit di media sosial menyatakan bahwa pentingnya menjaga *personal security* prajurit TNI dalam menggunakan media sosial untuk menjaga dari kebocoran data dan informasi yang dapat membahayakan keamanan nasional (Sutrisno, 2017). Untuk menambah khasanah penelitian yang sudah ada, penelitian ini menambah beberapa aspek kebaruan *(novelty)* yaitu (1) penelitian ini mengkaji bagaimana pentingnya aspek *Cyber Security Awareness* dalam melakukan aktivitas digital baik di ranah publik maupun militer, (2) penelitian ini mengkaji penggunaan *geo tagging* yang selama ini dianggap mempermudah aktivitas publik dalam aktivitas digital di sosial media khususnya instagram dan google maps bisa memberikan dampak yang membahayakan bagi keamanan nasional. (3) Penelitian ini mengkaji dampak penggunaan *geo tagging* terhadap keamanan nasional dari berbagai aspek ancaman baik fisik maupun non fisik.

2. METODE

Untuk mengkaji tulisan dalam penelitian ini menggunakan metode post positivisme (kualitatif) dengan pendekatan deskriptif. Penelitian deskriptif adaah penelitian yang bertujuan untuk menggambarkan fenomena melalui kata-kata, angka, klasifikasi dan garis besar untuk dapat menjawab pertanyaan siapa, kapan, di mana dan bagaimana terkait fenomena yang yang terjadi (Neuman, 2014). Pada penulisan artikel ini data dan fakta tentang mengenai peran negara dalam hak pemakanan akan dijabarkan secara deskriptif dengan sudut pandang *cyberpolitics*. Sementara itu untuk teknik pengumpulan data yang akan digunakan penulis dalam penelitian ini adalah menggunakan metode studi kepustakaan (literatur). Studi kepustakaan menurut Sugiyono adalah kajian teoritis dan referensi yang memiliki relevansi dengan nilai, budaya, dan norma yang berkembang pada fenomena sosial yang diteliti

(Sugiyono, 2013). Dalam penelitian ini penulis menggunakan data yang bersumber dari jurnal ilmiah, buku dan internet sebagai referensi.

Tinjauan Pustaka

Kesadaran Keamanan Siber (*Cyber Security Awareness*)

Security Awareness menurut Edward yaitu kemampuan dan pengetahuan seseorang dalam menggunakan media internet dan mengetahui pentingnya melindungi data pribadi atau kelompok (Afandi, Kusyanti, & Wardani, 2017). Pentingnya kesadaran akan keamanan siber diperlukan oleh semua pihak, salah satu hal yang harus disadari menurut Sarno dan Iffano dalam (Sutrisno, 2010) adalah aspek keamanan informasi yang terdiri dari 3 hal

1. Kerahasiaan *(Confidentiality)* hanya pihak yang berwenang untuk mengakses informasi.
2. Integritas *(Integrity)* data tidak diubah tanpa sepengetahuan pihak berwenang.
3. Ketersediaan *(Availability)* yaitu memastikan data tersedia saat dibutuhkan.

Selain Security Awareness, menurut beberapa ahli dalam penelitian Edwars, K. terdapat variabel- variabel lain yang mempengaruhi seseorang dalam berprilaku dalam menggunakan internet (Edwards, 2015) yaitu :

1. Kesadaran keamanan dapat memiliki efek positif pada efikasi diri keamanan karena pengguna yang sadar keamanan akan mengetahui teknologi dan prosedur yang tersedia untuk mencegah dan menghilangkan ancaman keamanan (Rhee et al., 2009)
2. Individu yang memiliki kesadaran akan nilai informasi memiliki kecenderungan untuk menuntut kontrol atas pengungkapan dan penggunaan informasi (Al Abri et al., 2009)
3. Pengguna Internet yang melek huruf memiliki kekhawatiran privasi yang lebih kuat karena pemahaman mereka tentang keseriusan, kerentanan, dan ketidakamanan Internet (Dinev & Hart, 2005)

Media Baru

Menurut Ganley dalam (Ward, 1995) menyatakan bahwa media baru membuat warga negara menjadi lebih informatif secara politis sehingga meningkatkan demokrasi atau biasa disebut citizen journalism. Sedangkan McQuail menyatakan bahwa media baru membuat komunikasi dua arah yang lebih interaktif untuk \menerima dan mengirim informasi secara bersamaan, sehingga dapat menimbulkan feedback atau dampak yang bervariasi (Wahid, 2016). Media baru memiliki beberapa karakteristik yang berbeda dengan media lama yaitu (Wahid, 2016) Packet Switcing, yaitu dapat mengirim audio, visual dan text secara bersamaan. Multimedia, yaitu pesan berupa audio, visual dan text dapat dikirim melalui berbagai saluran.

Interaktif, yaitu penerima dan pengirim pesan dapat berinteraksi secara langsung. Synchronicity, pertukaran informasi bebas ruang dan waktu dimana interaksi bisa dilakukan bersamaan (*synchronous communication*) dan tidak bersamaan (*Asynchronous communication*). Hypertextuality, cara memproduksi dan menyajikannya tidak secara sistematis urutan seperti text atau media kertas (Wood and Smith, 2005)

Sementara menurut Terry Flew (2002), media baru mempunyai karakteristik yaitu (Wahid, 2016) Manipulable, yaitu kapabilitas memanipulasi. Networkable, yaitu jaringan yang luas dan tidak terpenjara ruang. Dense, yaitu kapasitas yang besar dengan alat yang kecil. Compressible, yaitu dapat digabungkan. Impartial, yaitu pesan dan proses bersifat general untuk siapapun

Kehadiran media baru yang memiliki karakteristik khusus mendorong lahirnya beberapa aplikasi digital sebagai bagian dari media baru. Berbagai jenis dan fungsi media baru diantaranya media sosial Blog, Facebook, Twitter, Wordpress, Friendster, Myspace, Google+, Path, Instagram (Wahid, 2017). Namun tidak hanya media sosial terdapat beberapa jenis media baru untuk keperluan informatif di berbagai bidang seperti untuk perdagangan daring (e-Commerce), mesin pencari informasi (search engine), news aggregator, seperti Google, Yahoo, Bing, dan jasa penyaring berita (Prakoso Aji & Indrawan, 2019). Selain itu terdapat juga media baru lainnya yang berisi informasi lokasi dan penunjuk arah seperti Google Maps dan Waze.

Geo Tagging

Geotagging adalah proses pemberian informasi lokasi pada GPS berupa informasi titik koordinat latitude dan longitude pada foto digital (Defitria, dkk., 2018). *Global Positioning System* adalah sistem navigasi berbasis satelit yang awalnya digunakan oleh Departemen Pertahanan Amerika Serikat pada tahun 1978 (Ary, 2014). Untuk melakukan geotagging terdapat 3 (tiga) metode yang dapat dilakukan menurut Nandipati dalam (Defitria, U., dkk.2018) yaitu geocoding manual, yaitu dengan menginput titik koordinat. Kamera yang didalanya menggunakan teknologi GPS memiliki informasi. Kamera yang menggunakan teknologi GPS terpisah yang membutuhkan software tambahan untuk mengetahui informasi titik koordinat

Geotagging sendiri dapat digunakan untuk berbagai multidisiplin ilmu, menurut Firman Geotagging dapat digunakan untuk pemetaan kota dan politik seperti memetakan pergerakan pengguna media sosial, memetakan lokasi penting bagi pengguna media sosial, memetakan area yang paling banyak dilalui, memetakan pusat keramaian dan pusat kegiatan, menganalisis sebaran postinan pendukung politik (Firman, 2022). Perkembangan media sosial yang begitu

pesat dengan berbagai jenis dan fungsinya umumnya menggunakan geotagging sebagai salah satu feature nya. Berikut ini beberapa sosial media yang menggunakan geotagging atau disebut sebagai *geosocial* media (Han et al. (2019).

Data sets	Types	Data contents [a]					Platforms or datasets and paper numbers
		T	G	L	I	V	
Social Media Data Sets	social network sites	☑	☑	☑	☑	☑	Twitter(49);Facebook(2); Weibo(1);WeChat; Telgram; Tumblr
	image sharing sites		☑	☑	☑		Flickr(3); Instagram(1); Pinterest
	video sharing sites		☑	☑		☑	YouTube(2); Youku; Tiktok
	Forums or blogs	☑	☑	☑	☑		Reddit or the dark web(6)
	Game sites		☑			☑	Twitch; Steam
	others	☑		☑	☑		Ushahidi or RapidSMS, etc.(4)
	Security database	☑		☑			GDELT, MOD, AUTO, etc. (17)
Open Data Sets	Text corpus	☑					iWeb; WordNet; Google Web 1T
	Image/video labeled datasets				☑	☑	ImageNet; YouTube-8 M
	Geospatial datasets		☑	☑	☑		Geonames;OpenStreetMap; GDAM; GPW

[a]T is text, G is graph, L is location, I is image, and V is video. It means that the data sets have the corresponding data mainly if the table cell of data contents is checked.

Gambar 1. Penggunaan Geo Tagging

Sumber: Han et al. (2019)

Keamanan nasional

Konsep keamanan nasional menurut Tim Setjen Wantannas RI dilandaskan pada Pancasila sebagai falsafah bangsa yang diturunkan ke UUD 1945. Dalam melaksanakan keamanan negara ada dua konsep yang dijalankan yaitu konsep keamanan berbasis faham negara (*state centered security*) yaitu negara dapat menggunaan seluruh kekuatan dan sumber daya untuk menjamin keamanan negara. Selain itu negara juga menjalankan konsep (people centered security) yaitu bagaimana negara menjamin keamanan warganya. Konsep berikutnya yaitu Berdasarkan kondisi, keamanan nasional terbagi menjadi beberapa kondisi yang mempengaruhi hak dan kewajiban negara, publik warga negara dalam menjaga keamanan negara. (Tim Setjen Wantannas RI, 2010).

Berdasarkan ancaman terhadap keamanan nasional, terdapat 2 (dua) jenis (Tim Setjen Wantannas RI, 2010)

1. Pertama berdasarkan sumber datangnya ancaman, yaitu Ancaman Internal misalnya pemberontakan, terorisme, kecelakaan transportasi. dan ancaman eksternal misalnya invasi militer dari negara lain, keamanan warga negara di negara lain.

2. Kedua berdasarkan jenis ancamannya, yaitu ancaman fisik misalnya serangan militer, aksi teror, bencana alam, dan ancaman non fisik misalnya krisis ekonomi, kemiskinan, tingkat pendidikan yang rendah

Sedangkan untuk menjalankan keamanan nasional, maka terdapaat sistem keamanan nasional yang terdiri dari 3 (tiga) subsistem keaman nasional yaitu (Tim Setjen Wantannas RI, 2010):

1. Subsistem Keamanan Negara. Bertujuan untuk menjaga dan melindungi negara sebagai sebuah entitas politik yang meliputi kemerdekaan, kedaulatan negara, integritas teritorial, dan tegaknya konstitusi. Untuk mengatasi ancaman eksternal negara menggunakan subsistem pertahanan negara (*defence*), sedangkan untuk mengatasi ancaman internal negara menggunakan subsistem keamanan internal (*Internal security*).
2. Subsistem Keamanan Publik. bertujuan memberikan perlindungan keamanan kepada publik terhadap setiap ancaman atau segala sesuatu yang membahayakan kepentingan dan kebutuhan publik
3. Subsistem Keamanan Warga Negara bertujuan memberikan perlindungan keamanan kepada setiap warga negara Indonesia terhadap setiap ancaman atau segala sesuatu yang dapat membahayakan haknya untuk bebas dari rasa takut (freedom from fear), bebas untuk berkeinginan (freedom from want).

Semakin meningkatkan potensi ancaman dari dunia siber membuat negara harus melakukan startegy keamanan dari aspek siber. Keamanan siber adalah sebuah tindakan yang bertujuan memberikan proteksi dari ancaman, gangguan, serangan komputer, jaringan komputer, hardware, software, informasi dan elemen-elemen siber (Prakoso Aji & Indrawan, 2019). Keamanan Siber merupakan sebuah entitas yang sangat penting, sehingga negara memutuskan untuk membuat lembaga yang berfungsi untuk memastikan keamanan siber dengan memanfaatkan, mengembangkan dan mengonkonsolidasikan berbagai elemen yang terkait dengan keamanan siber nasional di lembaga BSSN pada tahun 2017.

Potensi-potensi ancaman keamanan siber pun semakin massive dan bervariasi, berikut beberapa potensi potensi ancaman keamanan siber menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber terbagi menjadi ancaman dan serangan. Berdasarkan perlakunya ancaman siber dapat di eksekusi oleh pihak yang mewakili dan diluar pemerintah. Adapun sumber-sumber ancaman siber diantaranya sumber internal dan eksternal, kegiatan Intelijen, kekecewaan, Investigasi, Organisasi Ekstremis, Hacktivists, Grup Kejahatan Terorganisir, Persaingan, Permusuhan &

KonflikTeknologi (Kementerian Pertahanan Republik Indonesia, 2014).

Berdasarkan aspek atau sumber yang membuat ancaman terjadi terbagi dari Ideologi, Politik, Ekonomi, Sosial, Budaya, Kebangsaan, Militer, Ilmu Pengetahuan dan Teknologi serta aspek lain yang terkait dalam kehidupan berbangsa, bernegara dan bermasyarakat termasuk kepentingan pribadi (Kementerian Pertahanan Republik Indonesia, 2014). Beberapa jenis ancaman siber yang ada diantaranya serangan *Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) bertujuan agar tidak dapat di akses dengan overloading kapasitas, *defacement* yaitu memodifikasi halaman web, *phishing* yaitu membuat website palsu dengan tujuan menarik data, Malware yaitu untuk mengganggu sistem dari komputer, Penyusupan siber yaitu masuk ke dalam sebuah sistem dengan cara Menebak sandi, Account yang tidak terlindungi, penipuan dan rekayasa Sosial, mendengarkan lalu lintas komunikasi data, trojan horse, sistemotentifikasi, cracking password terenkripsi, spionase, spam, penyalahgunaan protokol komunikasi. (Kementerian Pertahanan Republik Indonesia, 2014)

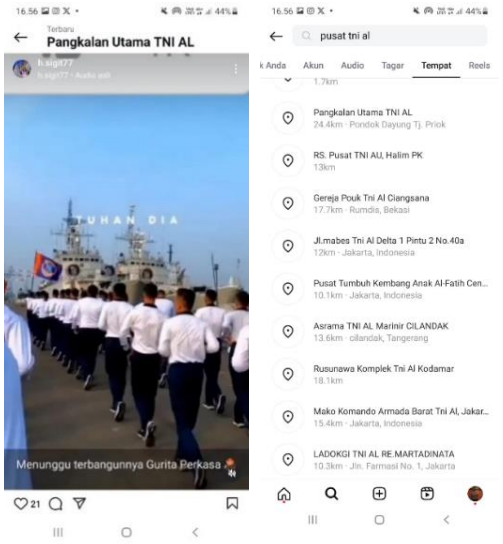
Selain ancaman, terdapat serangan siber. Serangan Siber (*Cyber Attack*) adalah ketika frekuensi dan eskalasi ancaman siber meningkat dan berubah dari ancaman yang bersifat potensial menjadi faktual. Berdasarkan sasaran, serangan siber terbagi menjadi tiga yaitu (1) Perorangan, masyarakat umum, organisasi, komunitas (2) Obyek vital infrastruktur kritis nasional *(National Critical Infrastructure*) (3) Kepentingan nasional, yaitu seluruh aspek yang terkait dengan tujuan nasional, lambang / simbol negara, politik negara serta kepentingan bangsa. Sementara serangan siber dapat berupa angguan fungsional, Pengendalian sistem secara remote., Penyalahgunaan informasi yang dapat menimbulkan kerusuhan, ketakutan, kekerasan, kekacauan, konflik (Kementerian Pertahanan Republik Indonesia, 2014)

3. HASIL dan PEMBAHASAN

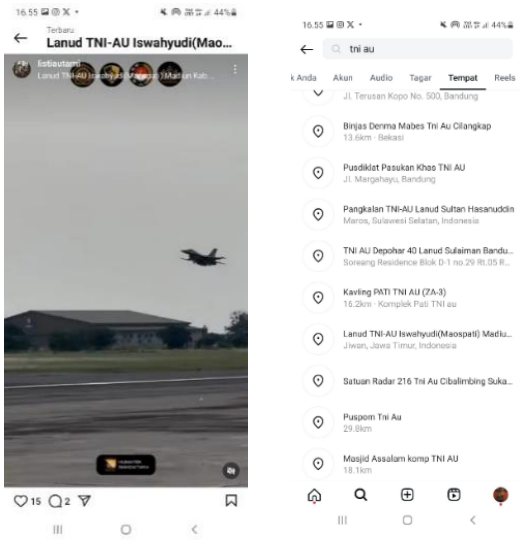
Narsisme sebagai bentuk rendahnya *Cyber Security Awareness*

Adanya budaya Narsisme dalam masyarakat Indonesia merupakan sebuah bentuk euforia dalam dinamika perkembangan siber di Indonesia. Narsisme sendiri merupakan sebuah prilaku menunjukkan personal life yang dapat menunjukkan aktivitas, kelebihan, kepopuleran, dengan tujuan mendapat respon berupa apresiasi dan perhatian dari orang lain. Budaya narsisme sering kali terkait dengan bagaimana prilaku seseorang dalam menggunakan media baru. Karakteristik media baru yang Interaktif (Wahid, 2016), membuat seseorang ingin mendapatkan respon atas setiap aktivitas digitalnya baik berupa foto, video dan berbagai macam konten lainnya.

Problemnya tidak selamanya budaya narsisme diiringi oleh unsur kKerahasiaan yang menjadi salah satu aspek penting dalam *Cyber Security Awareness* (Sutrisno, 2010).. Hal ini dapat kita lihat dari berbagai postingan warga dan apartur negara di media baru yang tidak mengedapankan hal tersebut. Banyaknya konten digital yang menggunakan geotagging untuk memperkuat narsisme seseorang. Salah satu contoh kasusnya dapat kita lihat dari banyaknya konten di Instagram yang menggunakan geotagging di objek-objek vital milik negara. Beberapa objek vital yang sering kali digunakan dalam geo Tagging misalnya pangkalan atau objek vital militer milik TNI. Markas atau tempat kegiatan militer menurut UU nomor 5 tahun 2018 masuk ke dalam kategori objek vital karena menyangkut pertahanan dan keamanan yang sangat tinggi (Kementerian Pertahanan Republik Indonesia, 2018). Berikut contoh bagaimana penggunaan geotagging di objek vital TNI.



Gambar 2. Geotagging TNI AL



Gambar 3.Geotagging TNI AU

Bila dikaji lebih dalam penggunaan Geotagging dalam konten media baru di objek vital tidak hanya dilakuan oleh masyarakat sipil yang awam terhadap objek vital, tetapi juga dilakukan apatur negara yang harusnya lebih memiliki kesadaran dan pengetahuan mengenai hal tersebut. Mengacu pada pemikiran Rhee bahwa kesadaran keamanan yang tinggi akan mengakibatkan efikasi positif pada diri yang mengakibatkan sadar akan pentingnya keamanan (Edwards, 2015). Contoh case di atas menandakan bahwa kesadaran keamanan siber masih rendah baik di ranah sipil maupun aparatur negara. Pada tahun 2016, Pusat Penerangan TNI AL pernah memberikan maklumat mengenai larangan bagi prajurit TNI untuk selfie di insatalasi militer dan alutista g yang kemudian di up-load lewat media sosial (Tentara Nasional Indonesia, 2017). Maklumat seperti ini juga disampaikan kembali pada tahun 2023, dimana

pada saat itu Panglima TNI Yudo Margono melarang prajurit TNI untuk melakukan selfie dengan simbol jari selama konstelasi Pemilu 2024.

Karakteristik media baru yaitu multimedia (Wahid, 2016) membuat budaya narsisme melalui selfie dengan *geo tagging* merupakan sebuah ancaman. Hal ini dikarenakan jenis konten yang dapat di upload dapat berupa video, foto, audio sehingga memperjelas pemetaan lokasi objek vital. Keamanan dalam melakukan upload konten pun terbuka, dimana siapapun yang menggunakan media baru dapat membuat konten. Beberapa media baru bahkan memberikan kewenangan bagi penggunanya untuk menambah, mengedit, menghapus tanpa permit dari pemilik lokasi. Bisa kita bayangkan dengan bebasnya seseoarang untuk dapat memvideokan berbagai alutista, denah markas militer. Meskipun praktiknya tidak mudah karena untuk memasuki kawasan militer tidak semua sipil punya akses namun di beberapa objek vital militer terbuka bagi sipil untuk menyelenggarakan beberapa kegiatan.

***Geo tagging* objek vital TNI ancaman masa depan**

Sistem geotagging yang ada dalam media baru dan integrasi dengan google maps melahirkan potensi ancaman yang baru bagi keamanan nasional dimasa yang akan datang. Beberapa ancaman yang penulis prediksi dapat terjadi digambarkan dalam bagan berikut ini

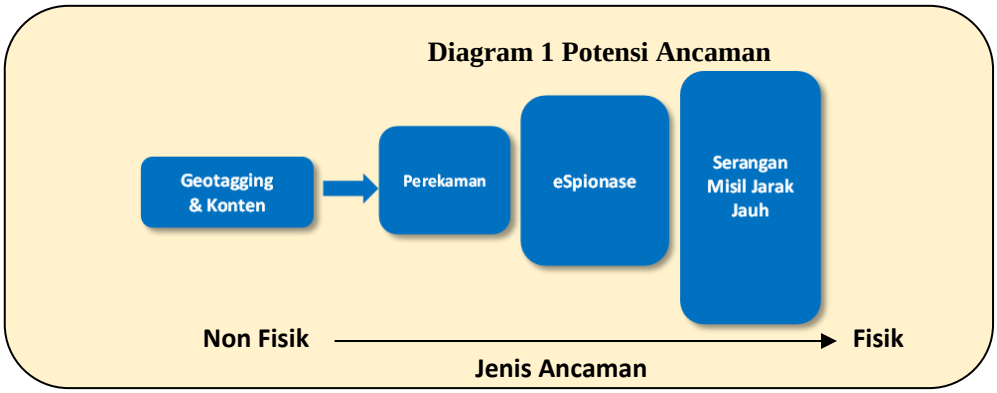


Diagram 1 Potensi Ancaman

Sumber: Dikelola Penulis, (2024).

Berdasarkan potensi ancaman terhadap keamanan nasional di atas, penulis akan mengkorelasikan dengan prinsip kerja geotagging dan bagaimana potensi ancaman masing-masing. Pertama, Perekaman. Adanya foto, street view, video, kordinat dalam media baru yang terhubung dengan google maps memungkinkan pihak asing atau pihak yang berkepentingan lainnya untuk melakukan perekaman big data sebagai sumber informasi. Keuda, *eSpionase*. Drone tak berawak (UAV)memiliki teknologi untuk dapat dijalankan secara otomatis dari jarak jauh berdasarkan titik kordinat yang dituju. Dalam konteks espionase, penggunaan drone belum termasuk dalam serangan fisik, namun masih serangan

non fisik. Kekuatan drone dianggap bisa menutupi kekurangan kemampuan dan resiko keamanan infiltrasi seorang intelejen. Terdapat 4 (empat) fungsi drone dalam kegiatan espionase yaitu ISRA (i*ntelligence, surveillance, reconnaissance and attack*) (Lesmana et al., 2023). Tentunya dapat kita bayangkan bagaimana jika semua titik kordinat objek-objek vital khususnya militer diketahui oleh pihak asing atau orang masyarakat yang bertindak sebagai agen. Penggunaan drone sebagai alat espionase sering digunakan oleh Amerika Serikat khususnya dalam berbagai operasi militer di Timur Tengah. Penggunaan drone sebagai alat mata-mata Bahkan dalam konteks olahraga pada Olimpiade 2024 lalu drone juga digunakan sebagai alat mata-mata

Ketiga, Serangan misil jarak jauh. Untuk menentukan sasaran lokasi tembak, rudal atau misil jarak jauh menggunakan sistem navigasi berupa koordinat atitude dan longitude yang di tentukan pada *Ground Control Station* (GCS) (Aria, Suteja, Gunawan, & Jatnika, 2019). Sehingga dengan hasil pemetaan titik koordinat atas objek vital negara, maka ancaman fisik atas serangan yang paling dikawatirkan yaitu serangan rudal atau misil jarak jauh bukan mungkin terjadi di Indonesia. Beberapa rudal atau misil jarak jauh yang ada di dunia saat ini misalnya RS-28 Sarmat milik Rusia dengan jarak tempuh 10 .000-18.000 kilometer, RS -36 (SS-18 Satan) milik Rusia dengan jarak tempuk 10.200-16.000 kilometer, DF-41 (CSS-X-20) milik China dengan jarak tempuh 12.000-15.000 kilometer. (Kompas, 2024). Hal ini semakin membukakan mata kita bahwa potensi perang lintas benua dengan menggunakan misil atau rudal jarak jauh semakin nyata.

5. SIMPULAN

Kesadaran keamaan siber merupakan salah satu aspek penting dalam menjaga keamanan nasional. Hal ini dikarenakan perkembangan teknologi digital banyak melahirkan media baru yang mempunyai beberapa feature unggulan seperti Geotagging. Penggunaan Geotagging dalam media baru sering kali didasari prinsip narsisme oleh seseorang, khususnya saat berada dalam objek-objek vital milik militer. Namun prilaku tersebut tidak hanya dilakukan oleh masyarakat sipil melainkan oleh aparatur negara.

Pengguaan Geotagging dalam media baru yang memiliki koneksi dengan aplikasi petunjuk wilayah seperti google maps mengakibatkan beberapa informasi penting mengenai objek vital dapat diketahui secara publik misalnya informasi titik koordinat, foto, video, street view. Hal tersebut merupakan ancaman bagi keamanan nasional karena dapat melahirkan potensi yang membahayakan keamanan seperti pemetaan wilayah, espionase, serangan misil atau rudal jarak jauh.

Kurangnya kesadaran akan keamanan siber dan ketidaktahuan bahaya menggunakan geotagging dalam media baru menurut penulis perlu segera dilakukan beberapa kebijakan penting seperti pelarangan bagi sipil dan militer untuk melakukan upload konten di area objek vital, pelarangan penggunaan geotagging pada objek vital, patroli siber yang berkesiambungan untuk memantau geotagging terhadap objek vital, perlunya angkatan siber yang kuat, terlatig dan didukung teknologi serta pendidikan akan kesadaran keamanan dan potensi akibat prilaku dalam melakukan aktivitas digital.

Saran dari penulis, perlunya regulasi yang mengatur bagaimana beraktivitas di objek vital milik negara khususnya TNI dan Polri, perlunya sosialisasi kepada aparatur dan warga sipil mengenai pentingnya *Cyber Security Awareness* dan sistem keamanan siber yang relevan dengan potensi ancaman terkini

6. DAFTAR PUSTAKA

Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis hubungan kesadaran keamanan, privasi informasi, dan perilaku keamanan pada para pengguna media sosial Line. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 1(9), 783-792.

Aria, M., Suteja, I. H., Gunawan, R., & Jatnika, I. (2019). Sistem navigasi berbasis waypoint untuk roket electric ducted fan (Navigation system based on waypoint for electric ducted fan rocket). Telekontran, 7(1), 42-52

BBC News. (2017, May 13). Massive ransomware infection hits computers in 99 countries. BBC. https://www.bbc.com/news/technology-39901382

Choucri, N. 2012. *Cyberpolitics in international relations*. Cambridge, MA: MIT Press

Defitria, U., Priyambadha, B., & Rusdianto, D. S. (2018). Pembangunan aplikasi social geotagging destinasi wisata berbasis android. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2(12), 6610-6617.

Edwards, K. (2015). E*xamining the security awareness, information privacy, and the security behaviors of home computer users* (Doctoral dissertation, Nova Southeastern University).

Firman Afrianto.2022. Jejak Digital Spasial di Media Sosial. Jakarta: Qiara Media

Han, Z., Li, S., Cui, C., Han, D., & Song, H. (2019). Geosocial media as a proxy for security: A review. IEEE Access, 7, 154224-154238.

Kementerian Pertahanan Republik Indonesia. 2014. Pedoman pertahanan siber. Jakarta : Kementerian Pertahanan Republik Indonesia

Kementerian Pertahanan Republik Indonesia. (2018). Undang-Undang Nomor 5 Tahun 2018 tentang Penanganan Tindak Pidana Terorisme. https://www.kemhan.go.id/itjen/wp-content/uploads/2018/10/uu5-2018bt.pdf

Kompas.com. (2024, April 19). 10 rudal balistik dengan jangkauan terjauh di dunia beserta negara. https://www.kompas.com/tren/read/2024/04/19/123000965/10-rudal-balistik-dengan-jangkauan-terjauh-di-dunia-beserta-negara.

Lesmana, D., Permana, Y., Santoso, B., & Infantono, A. (Tahun). Aplikasi drone militer dengan produk alutsista Indonesia untuk over the horizon operations (Military drone applications by using Indonesian defense equipment for over the horizon operations). Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Volume 3, Tahun 2021, hlm. 1-10

Mardani, A. (2014). Sistem informasi geografis pelaporan masyarakat (SIGMA) berbasis foto geotag. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 2(3), 118-123.

Neuman W., Lawrence.2014. Social Research Methods: Qualitative and Quantitative Approaches Seven Edition. Edinburgh: Pearson Education Limited

Nurahman, A., & Pribadi, P. (2023). Rudal Canggih dari Tiga Negara Superpower: JASSM, Kinzhal, dan DF-41. Bincang Sains Dan Teknologi, 2(01), 21–29. https://doi.org/10.56741/bst.v2i01.295

Nye, J. S. 2010. *Cyber power*. Cambridge, MA: Harvard University

Prakoso Aji, M., & Indrawan, J. (2019). Cyberpolitics: Perspektif baru memahami politik era siber. Depok: PT Raja Grafindo Persada.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2), 172-191.

Sarfaraz, O., Adil, M., GhayasUddin, M., Qadri, M. T., & Mohy-Ud-Din, Z. (2015). GPS Inertial Missile Guidance System.*Communications in Control Science and Engineering* (CCSE),3, 15-20

Sutrisno, B. T. (2017). Tantangan menjaga personal security prajurit di media sosial . DEFENDONESIA, 2(2), 1-8.

Tim Setjen Wantannas RI.2010. Keamanan Nasional Sebuah Konsep dan Sistem Keamanan bagi Bangsa Indonesia. Jakarta: Sekrtariat Jendral Dewan Keamanan Nasional

TNI. (2016, April 12). Hati-hati prajurit unggah foto di media sosial. TNI. https://tni.mil.id/view-94816-hati-hati-prajurit-unggah-foto-di-media-sosial.html

Umaimah Wahid. 2016. Komunikasi Politik Teori, Konsep, dan Aplikasi Pada Era Media Baru. Bandung: Simbiosa Rekatama Media

Valli, C., & Hannay, P. (2010, July). Geotagging Where Cyberspace Comes to Your Place. In Security and Management (pp. 627-632).

Wang, X., Zheng, Y., & Lin, H. (2015). Integrated guidance and control law for cooperative attack of multiple missiles. *Aerospace Science and Technology*,42, 1-11

Waskito, A. G., Nachrowie, N., & Suprayogi, S. (2017). Evaluasi Ketepatan Sasaran Roket Menggunakan Metode Polar. Prosiding SNATIF, 465-468.

Xu, M., Bu, X., Han, W., & Cao, Y. (2019). Dual-band infrared radiation for rotating missile attitude measurement and interference compensation. I*EEE Access*,7, 69326-69338