TANTANGAN MENJAGA *PERSONAL SECURITY* PRAJURIT DI MEDIA SOSIAL

B.T. Sutrisno SP [1]

Abstrak: Teknologi Media Sosial (Medsos) saat ini telah menjadi bagian yang tidak terpisahkan dari kehidupan masyarakat Indonesia, tidak terkecuali prajurit Tentara Nasional Indonesia (TNI). Penggunaan Medsos di kalangan prajurit disatu sisi sangat berguna sebagai media membangun jejaring dan menambah pengetahuan, namun disisi lain sangat riskan seiring besarnya potensi kebocoran informasi pribadi prajurit sebagai aktor pertahanan Negara yang dikenal dengan istilah *Personal Security (Persec)*. Metode penelitian yang digunakan adalah deskriptif dengan teknik pengumpulan data melalui studi pustaka dan penelusuran mendalam terhadap akun-akun prajurit TNI di Medsos, dengan objek penelitian adalah akun-akun prajurit TNI di Medsos. Hasil dari penelitian ini adalah: Markas Besar (Mabes) TNI sudah menerbitkan aturan terkait penggunaan Medsos di kalangan prajurit, namun masih banyak prajurit yang secara sengaja atau tidak sengaja membocorkan Persec melalui akun pribadinya melalui Medsos.

Kata kunci: *Media Sosial, Personal Security, Keamanan Personil, Pertahanan Negara*

1. PENDAHULUAN

Pesatnya perkembangan Teknologi Informasi yang salah satunya ditandai dengan hadirnya berbagai macam aplikasi Media Sosial (Medsos) berbasis jaringan internet merupakan keniscayaan yang tidak dapat di hindari. Penggunaan Medsos saat ini telah menjadi bagian dari gaya hidup *(lifestyle)* hampir di semua lapisan masyarakat Indonesia yang digunakan untuk membangun jejaring dan komunitas yang spesifik berdasarkan visi, misi, ide, gagasan, hobi, asal daerah, profesi, sampai dengan melebarkan jaringan bisnis secara luas dan cepat tanpa sekat pembatas lokasi dan waktu. Sebagai bagian dari masyarakat, tren penggunaan Medsos dalam kehidupan sehari-hari juga terjadi di kalangan prajurit Tentara Nasional Indonesia (TNI), yang tentunya mempunyai dampak positif dan negatif. Dampak positif dari penggunaan Medsos di kalangan prajurit diantaranya adalah memudahan prajurit menyampaikan atau mendapatkan informasi, mempermudah komunikasi, dan mendapatkan pengetahuan serta wawasan tentang pekembangan terkini secara global. Sedangkan dampak negatif dari penggunaan Medsos di kalangan prajurit salah satunya adalah semakin besarnya potensi kebocoran informasi pribadi prajurit yang seharusnya tidak dipublikasikan secara luas karena ditakutkan apabila informasi tersebut tersebar atau jatuh kepada pihak lawan akan dapat mendatangkan ancaman dan kerugian terhadap prajurit, keluarga prajurit, serta institusi TNI, sehingga diperlukan perhatian khusus untuk meminimalisir potensi kebocoran tersebut.

2. LANDASAN TEORI

Banyak definisi tentang Medsos tergantung dari sudut mana kita memandangnya. Salah satu yang menjadi rujukan adalah definisi menurut Kaplan dan Haenlein (2010)[2] dimana Medsos didefinisikan sebagai kelompok aplikasi berbasis internet yang dibangun di atas dasar ideologi dan teknologi berbasis web generasi kedua (Web 2.0) yang memungkinkan penciptaan dan pertukaran konten menggunakan jaringan internet dimana konten tersebut dihasilkan para penggunanya sendiri yang dikenal dengan istilah *User Generated Content* (UCG), yang kemudian diklasifikasi dalam enam jenis, yaitu:

1. Jenis proyek kolaborasi berbasis website yang mengizinkan penggunanya untuk mengubah,

[1] Penulis adalah pemerhati pertahanan di Lembaga Kajian Pertahanan untuk Kedaulatan NKRI "KERIS". Penulis dapat dihubungi melalui email denbambang@gmail.com

[2] Kaplan, Andreas M., Michael Haenlein., 2010. **Users of the world, unite! The challenges and opportunities of Social Media**. Business Horizons, 53(1), p.59-68

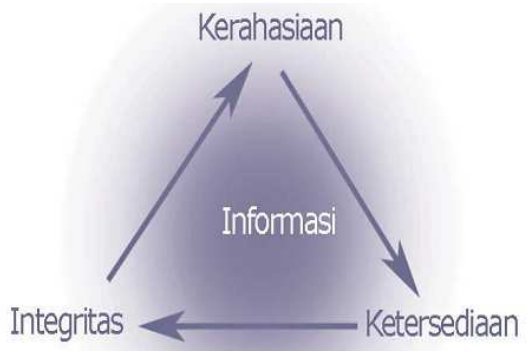
menambah, ataupun menghapus konten-konten yang ada di website tersebut. Contoh dari jenis Medsos ini adalah Wikipedia.

2. Jenis *blog* dan *microblog* yang memberikan keleluasaan bagi penggunanya dalam mengekspresikan sesuatu yang dirasakannya secara langsung dan terhubung dengan pengguna yang lain. Contoh dari jenis Medsos ini adalah Blogspot dan Twitter.
3. Jenis penyedia jasa pengelolaan konten dimana penggunanya dapat saling mengunggah, membagikan dan mengelola konten secara langsung baik konten berupa foto, video, dokumen, dan lain-lain. Contoh dari jenis Medsos ini adalah Youtube.
4. Jenis penyedia jejaring sosial yang mengizinkan penggunanya untuk terhubung secara personal dengan pengguna yang lain berdasarkan informasi spesifik seperti asal daerah, asal sekolah, hobi, pekerjaan dan lain-lain. Contoh dari jenis Medsos ini adalah Facebook.
5. Jenis *virtual game world* atau dunia permainan virtual yang memungkinkan pengguna dapat muncul dalam bentuk avatar-avatar yang diinginkan serta berinteraksi dengan orang lain selayaknya di dunia nyata. Contoh dari jenis Medsos ini adalah *Game Online*.
6. Jenis *virtual social world* atau dunia virtual yang penggunanya dapat merasa hidup di dunia virtual dan dapat berinteraksi dengan yang lain. Jenis ini hampir sama dengan *virtual game world* namun lebih bebas, serta lebih fokus pada kehidupan manusia sehari-hari. Contoh dari jenis Medsos ini adalah aplikasi Second Life.

Data adalah fakta mentah atau rincian dari sebuah peristiwa yang belum diolah, sedangkan informasi adalah hasil pengolahan data yang kemudian dapat digunakan untuk pengambilan sebuah keputusan. Oleh karena itu, informasi merupakan salah suatu aset penting dan sangat berharga dalam sebuah organisasi, sehingga diperlukan Sistem Manajemen Keamanan Informasi (SMKI) / *Information Security Management System* (ISMS) untuk menjaga keutuhan, ketersediaan, kerahasiaan, keaslian, dan mencegah penyalahgunaan informasi tersebut yang dapat merugikan organisasi. SMKI adalah sistem manajemen yang diterapkan untuk mengamankan aset informasi terhadap ancaman yang mungkin terjadi dan mengacu pada standar nasional yang dikeluarkan oleh pemerintah dan standar internasional (ISO/IEC 27001:2005).

Menurut Sarno dan Iffano (2009)[3], keamanan informasi *(information security)* adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis *(business continuity)*, meminimalisasi resiko bisnis (*reduce business risk)* dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Keamanan informasi terdiri dari tiga aspek yaitu:

1. Kerahasiaan *(Confidentiality)* yaitu aspek yang menjamin kerahasiaan data atau informasi, menjamin kerahasiaan atau informasi yang dikirim, diterima, dan disimpan, serta memastikan data atau informasi hanya dapat diakses oleh yang berwenang.
2. Integritas *(Integrity)* yaitu aspek yang menjamin data atau informasi tidak dirubah tanpa diketahui oleh yang berwenang, menjaga keakuratan dan keutuhan data atau informasi.
3. Ketersediaan *(Availability)* yaitu aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, dan memastikan pengguna yang berhak dapat menggunakan data atau informasi.



Gambar 1.
Elemen-elemen keamanan informasi

[3] Sarno, R. dan Iffano, I. 2009. **Sistem Manajemen Keamanan Informasi berbasis ISO 27001**. Surabaya: ITS Press

Keamanan informasi dapat dicapai dengan menerapkan beberapa bentuk strategi yaitu:

1. *Physical Security* (Physec) merupakan strategi yang fokus untuk mengamankan aset fisik organisasi
2. *Personal Security* (Persec) merupakan strategi yang fokus untuk mengamankan personil organisasi.
3. *Operasional Security* (Opsec) merupakan strategi yang fokus untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. *Communication Security* (Comsec) merupakan strategi yang fokus untuk mengamankan media dan teknologi komunikasi.
5. *Network Security* (Netsec) merupakan strategi yang fokus untuk mengamankan infrastuktur jaringan dan data organisasi.

Persec prajurit merupakan informasi terkait profil pribadi prajurit dalam kapasitasnya sebagai salah satu aktor penting dalam pertahanan sebuah Negara selain Alat Utama Sistem Senjata (Alutsista) dan dokumen-dokumen terkait Doktrin dan Strategi Pertahanan Negara. Beberapa informasi terkait diantaranya adalah pangkat, satuan, kualifikasi, alamat rumah, nomor telepon, email, dan informasi terkait keluarga prajurit seperti profil suami/istri, anak, famili, dan lain-lain.

4. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode penelitian deskriptif dengan tujuan untuk membuat deskipsi atau gambaran secara sistematis, faktual, dan akurat mengenai fenomena penggunaan Medsos di kalangan prajurit TNI dikaitkan dengan *Persec*. Menurut Sukmadinata (2006)[4], penelitian deskriptif adalah sebuah metode yang berusaha mendeskripsikan, menginterpretasikan sesuatu, misalnya kondisi atau hubungan yang ada, pendapat yang berkembang, proses yang sedang berlangsung, akibat atau efek yang terjadi atau tentang kecenderungan yang sedang berlangsung. Teknik pengumpulan data penelitian ini melalui studi pustakan tentang penggunaan Internet dan Medsos di Indonesia, serta penelusuran mendalam terhadap akun-akun prajurit TNI di Medsos, dengan objek utama penelitian adalah akun-akun prajurit TNI di Medsos.

5. PEMBAHASAN

5.1 Tren Penggunaan Internet dan Medsos di Indonesia

Pengguna internet di Indonesia dari tahun ke tahun semakin meningkat secara signifikan. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2016 jumlah pengguna internet di Indonesia telah mencapai 88,1 juta, dan 48 persen di antaranya merupakan pengguna internet harian yang mengakses internet menggunakan komputer, tablet dan ponsel[5]. Dari data jumlah tersebut, menurut data *We are Social* yang merupakan sebuah perusahaan riset dan pemasaran dari Singapura dalam laporannya berjudul *Digital in 2016*[6], jumlah pengguna aktif Medsos di Indonesia saat ini ada sekitar 79 juta dimana untuk penggunaan Medsos, aplikasi Facebook menjadi aplikasi nomor satu yang memiliki pengguna paling aktif di Indonesia kemudian disusul aplikasi Medsos lain seperti Twitter, Instagram dan Google Plus. Sedangkan untuk aplikasi *chatting*, aplikasi Blackberry Messenger (BBM) masih menjadi aplikasi dengan pengguna paling banyak di Indonesia kemudian disusul aplikasi WhatsApp dan Facebook Messenger yang dimiliki Facebook.

Berdasarkan informasi diatas, diketahui bahwa tren pengguna Medsos di Indonesia semakin meningkat seiring dengan pesatnya penggunaan Internet di masyarakat yang didalamnya juga termasuk prajurit TNI beserta keluarganya. Banyaknya penggunaan Medsos di kalangan prajurit TNI dapat dilihat dari semakin banyaknya akun pribadi prajurit

[4] Sukmadinata. 2006. **Metode Penelitian Pendidikan**. Bandung: Remaja Rosdakarya

[5] Liputan6, 2016.**3 Fakta Mengejutkan Pengguna Internet di Indonesia.**[online] Terdapat di: <http://tekno.liputan6.com/read/2435997/3-fakta-mengejutkan-pengguna-internet-di-indonesia> [Diakses 23 Oktober 2016].

[6] We are Social, 2016. **Special Reports Digital In 2016**. [pdf] We are Social. Terdapat di: <http://wearesocial.com/special-reports/digital-in-2016 > [Diakses 24 Oktober 2016].

TNI di Medsos seperti Facebook, Twitter, Instagram, Linkedin, Google Plus dan Medsos lain yang secara eksplisit menampilkan profilnya sebagai prajurit TNI. Penggunaan Medsos di kalangan Prajurit TNI sebenarnya tidak masalah selama tidak mempublikasikan data dan informasi terkait *Persec*, Alutsista yang dimiliki dan dioperasionalkan TNI, doktrin dan strategi, kemampuan, potensi serta kegiatan operasi yang sedang akan dilakukan, media komunikasi, teknologi komunikasi, jaringan komunikasi, struktur data, enkripsi, dan sandi yang berkaitan dengan tugasnya sebagai personil TNI. Selain itu karena Medsos sering menjadi tempat bertemunya berbagai gagasan dan ide para penggunanya, atau menjadi tempat membahas suatu peristiwa yang sedang menjadi perhatian di masyarakat, maka hendaknya prajurit TNI tidak menggunakan Medsos untuk menyampaikan tanggapan atas gagasan atau ide yang sedang menjadi bahan perhatian tersebut, apalagi yang bertentangan dengan sapta marga, sumpah prajurit dan delapan wajib TNI.

Menghindari perdebatan di Medsos terlebih yang terkait Suku Agama Ras dan Antar Golongan (SARA) juga penting dilakukan prajurit TNI karena bisa jadi perdebatan tersebut menjadi perselisihan bahkan bentrokan di dunia nyata. Berbagai organisasi dan perusahaan saat ini telah memasukan klausul tambahan tentang apa yang boleh dan apa yang tidak tidak boleh untuk di tulis atau diunggah oleh para anggota/pegawai di akun Medsos pribadinya, karena walaupun ditulis atau diunggah di akun dan atas nama pribadi, namun tetap saja sesuatu yang di tulis atau diunggah tersebut akan dikaitkan dengan organisasi atau perusahaan dimana anggota/pegawai tersebut bernaung, dan secara tidak langsung akan berdampak pada organisasi atau perusahaan. Untuk itu, sudah seharusnya TNI menerapkan hal yang serupa dengan menerapkan aturan yang ketat terkait penggunaan Medsos di kalangan prajurit agar tidak ada tulisan atau unggahan yang dilakukan prajurit di Medsos yang merugikan intitusi TNI dan pertahanan Negara.

5.2 Beberapa Pengaturan Penggunaan Medsos untuk Prajurit di Dunia

Tren menggunakan Medsos adalah sebuah keniscayaan yang tidak dapat di hindarkan pada era digital saat ini, namun mengingat besarnya efek yang ditimbulkan dari potensi kebocoran data dan informasi dari penggunaan Medsos di kalangan prajurit TNI, maka diperlukan peraturan yang ketat karena Medsos sejatinya memacu penggunanya untuk selalu *update* setiap saat. Hal tersebut yang sering memancing prajurit sengaja atau tidak sengaja mengunggah informasi-informasi yang seharusnya tidak diunggah secara bebas, semisal prajurit dengan sengaja atau tidak berfoto di depan Alutsista atau di lokasi yang seharusnya merupakan area terbatas *(restricted area)* dan mengunggahnya di akun Medsos pribadinya yang berakibat pihak lawan dapat menganalisa kemampuan Alutsista yang di miliki TNI berdasarkan foto yang di unggah tersebut.

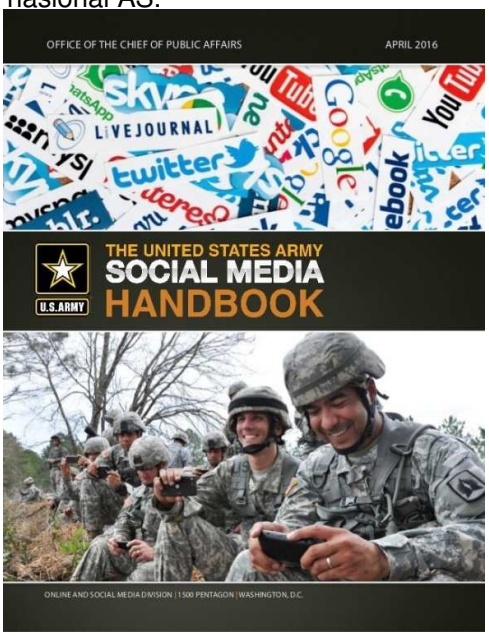
Beberapa Negara secara ketat mengatur penggunaan aplikasi Medsos oleh personil sipil dan militer yang terkait pertahanan, berikut beberapa contoh diantaranya:

a. Amerika Serikat

Sebagai Negara dengan angkatan bersenjata terlengkap dan tercanggih di dunia, Amerika Serikat (AS) secara khusus membuat aturan yang sangat detail tentang cara penggunaan dan pengamanan akun Medsos pribadi yang digunakan personil sipil dan prajurit yang bekerja di Departemen Pertahanan serta Militernya.[7] Selain itu, Militer AS bahkan memberikan pelatihan khusus kepada prajuritnya tentang cara yang aman menggunakan Medsos yang dilengkapi dengan buku panduan *(handbook)* dimana buku panduan tersebut terus di *update* seiring berkembangnya tren penggunaan jenis aplikasi Medsos di lingkungan prajurit. Buku panduan tersebut berisi contoh-contoh unggahan yang baik dan yang buruk dalam menggunakan Medsos serta cara mengamankan agar penggunaan

[7] Chief Information Officer, U.S. Department of Defense, 2017.**Web and Internet-based Capabilities (IbC) Policies**. [online] Terdapat di: <http://dodcio.defense.gov/DoD-Web-Policy [Diakses 6 Maret 2017].

Medsos tersebut tidak merugikan dan menjadi ancaman bagi keamanan nasional AS.[8]



Gambar 2.
Caver US Army Social Media Handbook 2016
Sumber: https://www.army.mil

b. Australia

Departemen Pertahanan Australia mulai mengatur penggunaan Medsos untuk personil sipil dan militer di Departemen Pertahanan dan Militer Australia dengan mengeluarkan *Defence Instructions (General)* DI(G) ADMIN 08-2 pada tahun 2013 yang kemudian di revisi dan disempurnakan pada tahun 2016.[9] Walau tidak sedetail dan selengkap yang di keluarkan oleh Departemen Pertahanan AS, DI(G) ADMIN 08-2 setidaknya memberikan petunjuk yang sangat jelas tentang apa yang boleh dan tidak boleh dilakukan oleh personil sipil dan militer di Departemen Pertahanan dan Militer Australia ketika menggunakan akun pribadi Medsosnya. Selain itu DI(G) ADMIN 08-2 juga mengatur tentang konsekuensi hukum yang akan di terima oleh personil sipil dan militer di Departemen Pertahanan dan Militer Australia jika membocorkan data dan informasi di Medsos.

c. Indonesia

Markas Besar (Mabes) TNI secara resmi mengeluarkan Surat Telegram Asisten Intelejen (Asintel) Panglima TNI nomor STR/58/2015 tertanggal 13 Februari 2015 dalam rangka mencegah timbulnya kerugian baik Institusi maupun personil TNI terkait penggunaan Medsos dikalangan prajurit TNI. Dalam Surat Telegram yang ditujukan kepada para Kepala Staf Angkatan dan Panglima Komando Utama Operasi (Kotamaops) TNI tersebut ditekankan agar prajurit TNI di semua tingkatan tidak menggunakan Medsos sebagai alat untuk menyampaikan pendapat yang bersifat menentang kebijakan Pemerintah maupun pimpinan TNI. Selain itu prajurit TNI dilarang mempublikasikan kegiatan atau aktifitas pribadi yang bersifat dinas, aktifitas kegiatan dinas, dan memberikan komentar di dalam Medsos terhadap situasi dan kodisi Ideologi, Politik, Ekonomi, Sosial dan Budaya (Ipoleksosbud) serta Militer dan Pertahanan (Milhan) yang berkembang di masyarakat apabila justru membawa kerugian dan merusak citra institusi TNI.

Gambar 3.
Panduan Penggunaan Medsos bagi Prajurit TNI AD
Sumber: Majalah Jayakarta Kodam Jaya
edisi ke XXVI Triwulan I TA 2016

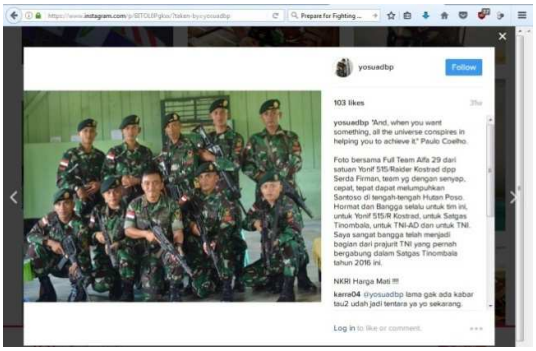
[8] U.S. Army, 2016. **The United State Army Social Media Handbook**. [pdf] U.S. Army. Terdapat di: <https://www.army.mil/e2/rv5_downloads/socialmedia/army_social_media_handbook.pdf> [Diakses 6 Maret].

[9] DEFGLIS, 2016. **Defence Instructions (General) DI(G) ADMIN 08-2 Use of social media by Defence personnel**. [pdf] DEFGLIS. Terdapat di: <https://www.defglis.com.au/resources/SocialMediaPolicy.pdf> [Diakses 6 Maret].

5.3 Contoh Kebocoran Persec Prajurit TNI di Medsos

Kurangnya pemahaman tentang cara menggunakan Medsos secara aman serta masih minimnya sosialisasi dan pembelajaran menggunakan Medsos di kalangan prajurit TNI khususnya di level paling bawah, menjadikan beberapa prajurit TNI secara sengaja atau tidak sengaja menggungah data dan informasi terkait Persec bahkan tugas operasi yang seharusnya dirahasiakan. Salah satunya dalam Operasi Tinombala Tahun 2016 yang merupakan operasi gabungan antara TNI dan Kepolisian Republik Indonesia (Polri) dalam upaya memburu dan menghancurkan jaringan teroris Mujahiddin Indonesia Timur (MIT) di Poso, Sulawesi Tengah. Seiring tersiar kabar tertembaknya Santoso yang merupakan pimpinan jaringan teroris MIT oleh prajurit TNI yang tergabung dalam Satuan Tugas (Satgas) Tinombala pada 18 Juli 2016, tidak lebih dari satu jam kemudian kronologi peristiwa baku tembak beserta satuan asal prajurit yang terlibat dalam peristiwa tersebut beredar luas di jejaring Whatsapp, BBM dan Facebook. Sehari kemudian, salah satu media berita *online* dalam Negeri juga memberitakan secara resmi peristiwa tersebut lengkap beserta kronologis disertai profil prajurit TNI yang terlibat beserta Nomor Registrasi Pokok (NRP), serta jabatan masing-masing prajurit di satuannya[10]. Tidak sampai disitu, beberapa hari kemudian foto lengkap prajurit TNI yang terlibat peristiwa tersebut juga di unggah di akun pribadi Instagram salah satu prajurit TNI yang juga menjadi bagian dari Satgas Tinombala.

Dari contoh kebocoran *Persec* prajurit TNI diatas, terlihat bahwa masih banyak prajurit TNI yang belum sepenuhnya memahami cara menggunakan Medsos secara aman dan masih suka "narsis", padahal tersebarnya informasi tersebut dapat berdampak serius bagi prajurit yang melaksanakan tugas operasi tersebut beserta keluarganya. Bisa dibanyangkan jika keluarga atau simpatisan jaringan teroris yang ditembak mati tersebut menaruh dendam dan berencana untuk melakukan balas dendam, maka informasi *Persec* yang dibocorkan di Medsos tersebut merupakan informasi yang pertama akan dicari untuk kemudian merencanakan serangan balasan terhadap prajurit, keluarga prajurit, atau satuannya.



Gambar 4.
Foto Personil Tim Alfa 29 Yonif 515/Raider Kostrad
Sumber : https://www.instagram.com/p/BITOL0Pgkxx/

Contoh lain kebocoran *Persec* yang juga menjurus kepada kebocoran kegiatan operasi (Opsec) sebagaimana ditunjukkan dalam gambar 5, dimana seorang prajurit TNI dengan sengaja menggungah foto kegiatan di kapal selam TNI saat sedang melaksanakan tugas operasi di akun Facebook pribadinya, padahal dengan mengunggah foto tersebut maka publik dan tentunya lawan dapat mengetahui kondisi dan posisi kapal selam TNI tersebut.

Gambar 5.
Foto Personil Kapal Selam TNI yang di unggah di Facebook
Sumber: https://www.facebook.com/photo.
php?fbid=466510463440962

Selain itu, dengan unggahan foto tersebut maka publik dan juga lawan dapat menelusuri lebih jauh profil rekan-rekan sesama prajurit kapal selam dalam jalinan pertemanan prajurit di akun Facebook pribadinya, dan sangat kontra produktif dan cenderung membahayakan pertahanan

[10]Tempo.co,2016. **Ini 9 Personel TNI yang Melumpuhkan Santoso**. [online] Terdapat di: <https://nasional.tempo.co/read/news/2016/07/19/058788864/ini-9-personel-tni-yang-melumpuhkan-santoso > [Diakses 3 Maret 2017].

Negara karena kapal selam merupakan salah satu Alutsista strategis dan seharusnya bersifat rahasia serta tidak terdeteksi keberadaannya.

Selain dua contoh diatas, berdasarkan penelusuran penulis masih banyak sekali ditemukan prajurit TNI yang menggunakan Medsos tidak memperhatikan kaidah-kaidah yang telah instruksikan oleh Mabes TNI, dengan tetap mengunggah foto *(selfie)* atau mengunggah berbagai kegiatan yang berkaitan dengan tugasnya sebagai prajurit TNI di akun Medsos pribadinya, seperti foto saat penugasan atau operasi, foto saat menggunakan Alutsista, menggunakan penanda lokasi *(geo-tagging)* ketika berada di markas atau saat pergeseran pasukan, mengunggah data pribadi yang seharusnya di rahasiakan seperti alamat rumah, nomor telepon, data keluarga, pangkat, satuan bahkan kualifikasi keahlian, padahal hal tersebut berpotensi mengakibatkan kebocoran *Persec*, serta merugikan Institusi TNI dan pertahanan Negara. Konsep aplikasi Medsos jejaring sosial seperti Facebook yang memungkinkan penggunanya untuk membangun jejaring secara spesifik berdasarkan deskripsi yang dimiliki oleh seseorang secara tidak langsung telah memberikan jalan untuk dapat mengetahui jaringan seseorang berdasarkan deskripsinya. Seorang prajurit TNI rata-rata mempunyai jaringan pertemanan di akun Facebook pribadinya yang juga prajurit TNI. Jika prajurit TNI tersebut tidak menggunakan Facebook secara aman dan benar, tidak memproteksi dan mengatur privasi akunnya sehingga publik dapat mengakses akun tersebut secara bebas, maka siapapun dapat melihat pola jaringan pertemanan, foto yang diunggah, dan aktifitas yang di unggah prajurit tersebut. Jika dahulu komunitas intelejen harus bersusah payah untuk mendapatkan data dan informasi *Persec* prajurit, maka bisa jadi saat ini untuk mengumpulkan data dan informasi *Persec* tersebut cukup dengan menganalisa akun Medsos para prajurit.

Persec prajurit sangatlah penting dalam pertahanan sebuah Negara, karena jika data atau informasi terkait *Persec* prajurit tersebut sudah terdokumentasi secara baik oleh lawan, maka bisa dibayangkan jika suatu saat terjadi perang, dan lawan telah menguasai data dan informasi terkait *Persec* prajurit dan menggunakan informasi tersebut untuk menebar ancaman dan teror, serta menyabotase prajurit atau keluarganya, maka dengan sendirinya secara psikologis semangat juang dan konsentrasi prajurit sebagai aktor pertahanan akan terganggu.

6. PENUTUP

6.1 Kesimpulan

Hadirnya aplikasi Medsos merupakan keniscayaan yang tidak dapat di hindari di era digital saat ini. Prajurit merupakan salah satu aktor penting dalam pertahanan Negara, sehingga informasi terkait prajurit sangat penting untuk dijaga keamanannya. Markas Besar (Mabes) TNI sudah menerbitkan aturan terkait penggunaan Medsos di kalangan prajurit, namun masih banyak prajurit yang secara sengaja atau tidak sengaja membocorkan data dan informasi terkait *Persec* melalui akun Medsos pribadinya, sehingga diperlukan sinergi antar *stakeholder* terkait pertahanan Negara untuk merumuskan pengaturan yang lebih detail terkait penggunaan Medsos di kalangan prajurit untuk meminimalisir potensi kebocoran data dan informasi tersebut. Tugas Pemerintah, *stakeholder* terkait pertahanan Negara, dan kemauan prajurit untuk menerapkan *sense of security* terhadap data dan informasi terkait pertahanan Negara merupakan sebuah keharusan di era digital, karena seiring perkembangan teknologi informasi dan komunikasi saat ini, data dan informasi dapat dengan cepat dan mudah tersebar secara luas. Banyak yang beranggapan Negara yang lebih maju dan menguasai teknologi yang lebih canggih pasti mengetahui semua data dan informasi di Negeri ini, tapi hal tersebut tidak sepenuhnya benar karena pada kenyataannya banyak data dan informasi yang beredar tersebut justeru secara sengaja atau tidak sengaja di unggah atau publikasikan sendiri oleh yang mempunyai data dan informasi tersebut, salah satunya dengan menggunakan Medsos.

6.2 Saran

Terdapat beberapa hal yang penulis sarankan terkait pengaturan penggunaan Medsos di kalangan prajurit, yaitu:

2.1. Kementrian Pertahanan (Kemhan) bersama dengan *stakeholder* terkait (Kemenko Polhukam, Kemenkominfo, BIN, Lemsaneg, Mabes TNI, dan Mabes Angkatan) hendaknya bersinergi dalam merumuskan dan membuat peraturan atau kebijakan tentang tata cara penggunaan Medsos di kalangan prajurit TNI dan personil sipil terkait pertahanan Negara.

2.2. Mabes TNI perlu membuat buku panduan *(handbook)* penggunaan Medsos yang aman untuk prajurit dan keluarganya. Buku tersebut hendaknya juga dilengkapi dengan contoh-contoh bentuk unggahan yang benar dan aman di Medsos, minimal di aplikasi Medsos yang paling banyak digunakan oleh prajurit seperti Facebook, Twitter, Path dan Instagram. Selain itu, buku panduan tersebut juga menjelaskan cara mengamankan *account* pribadi dan keluarga prajurit dalam kaitannya mencegah kebocoran data dan informasi terkait pertahanan Negara, semisal tidak asal menggunakan jaringan internet yang tidak aman, mengatur privasi di *account* Medsos, mengatur pola jejaring untuk Medsos berbasis jejaring seperti Facebook agar pola pertemanan dan diskrispi diri tidak diketahui publik, dan memastikan penanda lokasi *(geo-tagging)* dalam posisi tidak aktif *(disable)* di perangkat yang digunakan prajurit.

2.3. Mabes TNI dan Mabes Angkatan perlu melakukan sosialisasi secara menyeluruh dan berkelanjutan kepada prajurit TNI beserta keluarganya tentang cara menggunakan Medsos secara aman.

DAFTAR PUSTAKA

Militaryspot, 2014. **OPSEC and PERSEC**. [online] terdapat di: < http://www. militaryspot.com/resources/opsec-and-persec> [diakses 20 April 2017].

International Organization for Standardization, 2015. **ISO/IEC 27001:2005**. [online] terdapat di: <https://www.iso.org/standard/42103.html> <diakses 20 April 2017>

Sarno, R. dan Iffano, I. 2009. **Sistem Manajemen Keamanan Informasi berbasis ISO 27001**. Surabaya: ITS Press

Kaplan, Andreas M., Michael Haenlein., 2010. ***Users of the world, unite! The challenges and opportunities of Social Media***. Business Horizons, 53(1), p.59-68

Sukmadinata. 2006. **Metode Penelitian Pendidikan**. Bandung: Remaja Rosdakarya

Liputan6, 2016.3 **Fakta Mengejutkan Pengguna Internet di Indonesia**.[on line] Terdapat di: <http://tekno.liputan6.com/read/2435997/3-fakta-mengejutkan-pengguna-internet-di-indonesia> [Diakses 23 Oktober 2016].

We are Social, 2016. ***Special Reports Digital In 2016***. [pdf] We are Social. Terdapat di: <http://wearesocial.com/special-reports/digital-in-2016 > [Diakses 24 Oktober 2016].

Chief Information Officer, U.S. Department of Defense, 2017.***Web and Internet-based Capabilities (IbC) Policies***. [online] Terdapat di: <http://dodcio.defense.gov/DoD-Web-Policy [Diakses 6 Maret 2017].

U.S. Army, 2016. ***The United State Army Social Media Handbook***. [pdf] U.S. Army. Terdapat di: <https://www.army.mil/e2/rv5_downloads/socialmedia/army_social_media_handbook.pdf> [Diakses 6 Maret].

DEFGLIS, 2016. ***Defence Instructions (General) DI(G) ADMIN 08-2 Use of social media by Defence personnel***. [pdf] DEFGLIS. Terdapat di: <https://www.defglis.com.au/resources/SocialMediaPolicy.pdf> [Diakses 6 Maret].

Tempo.co,2016. **Ini 9 Personel TNI yang Melumpuhkan Santoso**. [online] Terdapat di: <https://nasional.tempo.co/read/news/2016/07/19/058788864/ini-9-personel-tni-yang-melumpuhkan-santoso> [Diakses 3 Maret 2017].