

DEWAN PERTIMBANGAN PRESIDEN

# WARTA



ISSN 2098-1975

9 772088 197563

#edisi 2. 2018

**PERKEMBANGAN  
ANCAMAN  
PERTAHANAN**

## WARTA WANTIMPRES

Warta WANTIMPRES merupakan media publikasi dwi bulanan yang bertujuan untuk menyampaikan profil dan kegiatan Wantimpres kepada publik secara berkala.

**Penanggung Jawab**  
Subiyantoro

**Pimpinan Redaksi**  
M. Arfan Sahib Sali K.

**Editor**  
Untung Widodo  
Veri Nurhansyah T.

**Penyusun**  
Andhi Ilham P.  
Aris Munandar  
B. Bonnik Manoe  
D. Herdiyan  
Dian Kartika Putri  
Fikroh Amali F. A.  
Syahlarriyadi

[www.wantimpres.go.id](http://www.wantimpres.go.id)

### FOKUS



**Subagyo Hadisiswoyo**  
Anggota  
Dewan Pertimbangan Presiden

"Perkembangan  
Ancaman Pertahanan"

### PERSPEKTIF



**M. Yusuf Kartanegara**  
Anggota  
Dewan Pertimbangan Presiden

"Ancaman Narkoba  
dan Pertahanan Nonmiliter"



**Gildas D. Lumy**  
Pakar Keamanan  
Teknologi Informasi

"Risiko Keamanan  
Aplikasi Pesan Instan"

### DAFTAR ISI

01 FOKUS

02 PERSPEKTIF

06 GALERI KEGIATAN

**Alamat Redaksi :**  
Jalan Veteran III No 2 Jakarta 10110  
Telp.: (021) 3444801  
Faks: (021) 3865092  
email: veri.nurhansyah@setneg.go.id



Hak Cipta dilindungi Undang - Undang.  
Dipersilahkan mengutip atau memperbanyak  
sebagian majalah ini dengan seizin tertulis dari  
penulis dan/atau penerbit.

Copyright © 2018

Foto Cover :



[www.pinterest.com](http://www.pinterest.com)  
© Creative Common License

# FOKUS

## PERKEMBANGAN ANCAMAN PERTAHANAN

**Jenderal TNI (Purn) Subagyo Hadisiswoyo**  
Anggota Dewan Pertimbangan Presiden

Perkembangan dimensi ancaman pertahanan yang dihadapi setiap negara semakin meluas dan melebar. Hal ini didorong oleh menyatunya serangan maupun pertahanan dengan aspek sosial, budaya, ekonomi, maupun aspek lain. Di sisi lain, kekuatan militer secara fisik mungkin hanya akan digunakan untuk menginvasi total, menguasai, dan menduduki wilayah suatu negara.

Menurut Jenderal TNI (Purn) Subagyo Hadisiswoyo, Anggota Wantimpres, seiring berkembangnya dimensi ancaman pertahanan, maka kesiapan kekuatan militer suatu negara masih menjadi deteren yang ampuh apalagi jika ditunjang dengan kemampuan menghadapi serangan siber sebelum melakukan operasi militer. "Dalam operasi militer, kecepatan dan pendadakan merupakan kunci kemenangan," kata beliau kepada *Warta Wantimpres*.

Permasalahannya, untuk mewujudkan kondisi militer yang selalu siap tersebut dibutuhkan anggaran besar dan peralatan yang mampu beroperasi di berbagai situasi. Pada sekarang ini, Amerika Serikat (AS) merupakan satu-satunya negara dengan kekuatan militer yang siap melakukan operasi setiap saat dan ke berbagai penjuru dunia. Jika melihat kondisi dalam negeri, kekuatan dan kemampuan militer Indonesia masih pada taraf kekuatan dasar minimal dengan anggaran masih di bawah 1% dari Produk Domestik Bruto (PDB). Secara teori, jumlah ini masih di bawah harapan lantaran idealnya anggaran militer suatu negara minimal 1,5% dari total PDB.

Foto : Saddra F.

Di sisi lain, Indonesia juga menghadapi ancaman nonmiliter yang terbilang kompleks. Indonesia dinilai oleh Jenderal TNI (Purn) Subagyo Hadisiswoyo sangat memerlukan lembaga yang mengkoordinasikan berbagai bentuk ancaman nonmiliter. "Kita belum terkoordinasi dalam menghadapi ancaman nonmiliter karena payung hukumnya belum diratifikasi ke dalam Undang-Undang Keamanan Nasional," ujar beliau.

Ancaman nonmiliter ini terus meningkat terutama salah satunya didorong oleh kepentingan ekonomi setiap negara. Saat ini, masing-masing negara ingin menguasai seluruh akses perhubungan, baik darat, laut, maupun udara, guna mengakumulasi keuntungan perdagangan semaksimal mungkin.

Permasalahannya, penguasaan akses tersebut seringkali dilakukan secara tidak berimbang. AS misalnya, sering mengklaim pentingnya penyiapan akses perdagangan untuk kepentingan internasional. Namun, apabila ada negara lain ingin memasuki aksesnya, AS akan menolaknya karena faktor kedaulatan negara. Kebijakan tidak berimbang ini akhirnya ditiru oleh banyak negara sehingga rentan menimbulkan konflik dan benturan. Oleh karena itu, perlu adanya standar internasional yang mengatur penguasaan akses ini agar menjadi norma bersama guna mencegah konflik antarnegara (VN).



**Letjen TNI (Purn) M. Yusuf Kartanegara, S.H.**  
 Anggota Dewan Pertimbangan Presiden

## ANCAMAN NARKOBA DAN PERTAHANAN NONMILITER

Seiring perkembangan zaman, ancaman yang dihadapi Bangsa Indonesia tidak lagi menyangkut serangan militer. Pada saat sekarang dan masa yang akan datang, Indonesia justru akan lebih sibuk bergulat dengan ancaman-ancaman yang sifatnya nonmiliter seperti peredaran gelap narkoba, korupsi, radikalisme, kejahatan siber, bencana alam, wabah penyakit, serta perdagangan manusia.

Menurut Letjen TNI (Purn) M. Yusuf Kartanegara, S.H., Anggota Wantimpres, penyalahgunaan narkoba merupakan ancaman terbesar yang menjadi musuh nomor satu Bangsa Indonesia dewasa ini. Hal ini dikarenakan begitu besarnya dampak negatif yang ditimbulkan oleh barang haram tersebut, mulai dari korban jiwa, kerugian harta benda, hingga dampak psikologis yang dapat menghancurkan generasi bangsa.

“Peredaran narkoba juga sudah sangat masif dan melibatkan semua lapisan masyarakat baik vertikal maupun horizontal,” kata beliau kepada *Warta Wantimpres*. Hal ini terbukti dari data Badan Narkotika Nasional (BNN) tahun 2016, jumlah pengguna narkoba di Indonesia sudah menyentuh angka 6 juta orang yang berasal dari berbagai kalangan usia dan profesi. Tak hanya itu, korban jiwa akibat penyalahgunaan narkoba mencapai 40-50 orang meninggal dunia per hari. Dari sisi material, kerugian negara akibat narkoba mencapai Rp 63,1 triliun.

Begitu masifnya penyalahgunaan narkoba dewasa ini menuntut seluruh elemen bangsa untuk bahu membahu melawan ancaman nirmiliter terbesar Indonesia tersebut. Upaya melawan bahaya narkoba tersebut sudah digaungkan Presiden Joko Widodo yang pada

tahun 2015 telah menyatakan Indonesia sedang mengalami status darurat narkoba. Pernyataan Presiden tersebut perlu diimplementasikan secara nyata dengan memperkuat sinergitas antara kementerian/lembaga terkait dan ditopang oleh dukungan SDM maupun anggaran yang memadai.

Sesuai dengan amanat Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, khususnya Pasal 7 Ayat (3) dan Pasal 19, tanggung jawab dalam menghadapi ancaman nirmiliter, termasuk ancaman narkoba, berada pada kementerian dan lembaga di luar bidang pertahanan, yakni Kementerian Kesehatan, Kementerian Hukum dan HAM, Kementerian Keuangan, Polri, BNN, Badan Pengawas Obat dan Makanan (BPOM), dan Badan Intelijen Negara (BIN).

Letjen TNI (Purn) M. Yusuf Kartanegara, S.H., menyatakan, peran serta BIN harus diperkuat guna melakukan deteksi dini dan cegah dini kemungkinan masuknya narkoba ke Indonesia. “Pemerintah dapat pula mempertimbangkan dan mengoptimalkan pelibatan TNI dalam membantu penanggulangan narkoba dengan tetap berpedoman pada undang-undang dan peraturan yang berlaku,” ujar beliau.

Partisipasi masyarakat juga harus terus dipupuk melalui kegiatan sosialisasi dan penyuluhan, serta memanfaatkan peran serta kelompok atau organisasi masyarakat. Hal ini diperlukan agar masyarakat turut tergerak guna bersama-sama membangun ketahanan terhadap bahaya penyalahgunaan narkoba (VN).

# RANAH BARU PERANG SIBER

## A. Chasib

Perkembangan internet setelah tiga dekade tidak terbendung, sistem komputer yang awalnya diciptakan untuk kepentingan militer semakin banyak penggunanya apalagi setelah terhubung dengan internet. Sejak saat itu dikenalkan "logic bomb" kendali siber yaitu bom yang dapat diledakkan dari jarak jauh bahkan untuk memadamkan listrik dari jarak jauhpun dapat dilakukan. Seorang teroris atau peretas bila melakukan serangan siber dapat mengacaukan sistem keuangan dengan merusak dinding sistem komputer bank. Karena kemampuan merusak yang dahsyat dan efisien itulah maka banyak dipilih untuk digunakan dalam melakukan serangan, termasuk untuk kepentingan militer.

Selama ini kita hanya mengenal ranah peperangan di empat domain yaitu darat, laut, udara dan ruang angkasa, namun dengan munculnya siber yang menggunakan domain tersendiri maka ranah peperangan bertambah yaitu ranah perang siber. Untuk mengantisipasi lebih awal, Amerika Serikat (AS) secara cepat menyiapkan infrastruktur dan menjadikannya ranah sebagai aset strategis nasional karena menyadari akan kemanfaatannya dan risiko di berbagai bidang. Banyak yang bertanya seperti apa perang siber itu? Dijelaskan oleh Richard Clarke dengan ilustrasi yaitu "bayangan perang yang dapat membawa bencana hanya dalam waktu 15 menit". Metodenya dengan mengirim Virus computer (*bugs*) sebagai penyebab rusaknya sistem kontrol, virus yang menginfeksi sistem dapat merusak berbagai kontrol sistem termasuk sistem data bahkan dapat merusak sistem kerja satelit sebagai kontrolernya.

Perang siber pada kenyataannya merupakan bagian dari evolusi *warfare* konvensional, yang berhubungan dengan aspek sosial secara luas dan perubahan politik. Permasalahannya adalah bagaimana menganulir ancaman yang menggunakan siber/teknologi komputer di mana tidak diketahui kapan dan siapa pelakunya, tiba-tiba terjadi kerusakan data atau kerusakan sistem komputer. Pertahanan terbaik melawan ancaman siber sampai saat ini adalah membiasakan masyarakat menerapkan prosedur pemberitaan, memahami bagaimana mengorganisir ancaman siber sehingga pengelolaan *database* aman. Serangan siber juga memberi dampak sosial cukup besar disamping kejahatan fisik. Sering timbul pemahaman keliru bahwa

serangan siber hanya ditujukan untuk perangkat militer saja padahal siber dapat menyerang segala bidang aspek kehidupan bermasyarakat, berbangsa dan bernegara.

Risiko lanjut akibat siber dapat menimbulkan kekhawatiran masyarakat dunia karena kerusakan industri pangan yang membawa konsisi masyarakat pada kesulitan pangan, kekacauan *currency* bahkan kekurangan uang, sementara pelakunya tetap menjadi misteri. Serangan siber sama bahayanya dengan serangan nuklir, oleh karenanya perang siber akan menjadi ranah perang baru mendatang. Keberadaan siber dapat dikatakan berkah di satu sisi karena untuk melakukan pertempuran tidak lagi memerlukan *hardware* yang besar dan banyak sementara disatu sisi bisa jadi malapetaka karena hanya dengan menekan tombol dapat menimbulkan kehancuran.

Internet disiapkan untuk kemudahan dan lebih riil tetapi tidak aman artinya bahwa pengguna dapat melakukan apa saja. Hampir 130 juta *email* per hari dikirim termasuk spam dimana sekitar 20 juta berisikan *scam* yang menyerang penerima untuk mendapatkan data-data atau sandi terutama pada sistem keuangan atau perdagangan. Pelepasan *malware* yang beredar berusaha mencuri sandi atau membuka sistem komputer untuk mengambil data dari luar. Penetrasi terus dilakukan guna merusak atau mengelabui sistem yang pada akhirnya sistem akan lumpuh sebelum digunakan. Karena tingkat pencapaian sasaran sangat besar maka kemampuan siber dapat berperan sebagai deteren, memang tidak begitu jelas pemisahan antara perang dan tindakan kriminal serta tidak jelas penyerangnya tetapi penggunaan siber tidak membuat sampai terjadinya kiamat elektronik.

Banyak contoh penggunaan serangan siber untuk melumpuhkan berbagai peralatan canggih sekalipun termasuk mengatasi peluru kendali, kejadian pelepasan "Stuxnet Worm" oleh Israel dan Amerika yang melumpuhkan sistem kontrol fasilitas nuklir Iran salah satu bukti ketajaman serangan. Perang atau serangan siber tidak di-*declare*, metoda penyerangan tidak langsung dapat dan sering dilakukan dengan melekatkan *chip*/alat elektronik pada suatu produk yang kemudian membagi data dengan pemilik produk.

Dengan demikian semakin jelas bahwa perang siber dapat dilakukan ke berbagai sasaran dengan berbagai media, serta membentuk domain baru yang menjadi ranahnya. Negara yang tidak menyiapkan pertahanan siber akan menjadi korban serangan langsung atau tidak langsung baik untuk pencarian data atau perusakan sistem. Jadi sudah selayaknya bagi Indonesia membentuk Badan Siber Nasional.

## RISIKO KEAMANAN APLIKASI PESAN INSTAN

Gildas D. Lumy  
Pakar Keamanan Teknologi Informasi

Penggunaan aplikasi layanan pesan instan (*instant messaging*) di Indonesia sangat masif. Hal ini setidaknya tercermin dari survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) yang dilakukan pada 2017. Sekitar 89,35% dari 2.500 responden yang disurvei mengaku telah menggunakan aplikasi pesan singkat untuk berkomunikasi. Temuan ini lebih tinggi dari tingkat penggunaan media sosial (87,13%) dan pemanfaatan layanan mesin pencari (74,85%).

"Kemudahan penggunaan selalu berbanding terbalik dengan faktor keamanan informasi," kata Bapak Gildas D. Lumy, Pakar Keamanan Teknologi Informasi kepada *Warta Wantimpres*. Hal ini juga didorong oleh model bisnis pesan layanan instan yang menuntut akuisisi pengguna sebanyak dan secepat mungkin. Alhasil, tidak semua pembuat aplikasi pesan instan melektakkan aspek keamanan sebagai prioritas utama.

Isu keamanan yang paling sering menjadi perbincangan dari penggunaan layanan pesan instan adalah potensi kebocoran informasi rahasia. Kebocoran ini disebabkan oleh beberapa faktor seperti informasi pesan yang tidak dienkripsi, pengguna kehilangan perangkat, fungsi pengelolaan keamanan grup yang minim, modus pencurian tampilan layar (*screen logger*), proses enkripsi/dekripsi pesan oleh server, salinan kunci enkripsi yang disimpan server, serta model bisnis penyedia layanan berbasis penambangan data pengguna.

Namun, tingginya risiko kebocoran informasi tersebut bukan berarti masyarakat tidak boleh menggunakan layanan pesan instan. Bapak Gildas D. Lumy menyarankan agar pengguna harus menggunakan aplikasi pesan instan yang model bisnisnya memprioritaskan aspek keamanan dan privasi. Ini dapat tercermin dari misalnya dari kode sumber aplikasi yang terbuka sehingga dapat dilakukan audit secara mendalam terutama dalam proses enkripsi/dekripsi data, serta pengelolaan kunci enkripsi.

Aplikasi yang baik juga harus memiliki proses enkripsi yang selalu aktif, bukan diaktifkan secara manual oleh pengguna. Hal ini mesti ditunjang pula dengan proses enkripsi *end-to-end* setiap pesan, termasuk dalam grup, sehingga hanya pengirim dan penerima yang dapat melihat pesan, sedangkan server hanya bertindak sebagai pengirim. Layanan pesan instan mesti pula memiliki fungsi pencegahan pencurian layar oleh *malware*, serta dapat menghapus pesan otomatis di ponsel pengirim dan penerima sesuai waktu yang ditetapkan pengirim.

Kendati begitu, bukan berarti aspek keamanan ini harus mengikis kenyamanan pengguna. "Aplikasi pesan instan justru harus diusahakan semaksimal mungkin keamanannya secara kompleks dan otomatis, tanpa dirasakan oleh pengguna," ungkap beliau. (AM, AIP, VN)



1



2



3



4



5



6



GALERI KEGIATAN

1. Bapak Suharso Monoarfa, Anggota Wantimpres, melakukan pertemuan dengan Kepala Badan Siber dan Sandi Negara (BSSN) dan pihak terkait lainnya, guna membahas tema "Penyelenggaraan Telekomunikasi Khusus oleh dan untuk Instansi Pemerintah, termasuk Pertahanan dan Keamanan Negara", di Kantor Wantimpres, Senin, 19 Maret 2018.
2. Ibu Sri Adiningsih, Ketua Wantimpres, didampingi oleh Ibu Erna Maria Lokollo, Sekretaris Anggota Wantimpres Ibu Sri Adiningsih, dan Bapak Maksum Isa, Sekretaris Anggota Wantimpres Bapak A. Malik Fadjar dan Tim Kajian Ketua Wantimpres "Perkembangan Ekonomi Digital dan Ekonomi Kreatif" mengunjungi *Bandung Creative Hub* dalam rangkaian kunjungan kerja ke Kota Bandung, Jawa Barat, Rabu, 21 Maret 2018.
3. Anggota Wantimpres, Bapak Subagyo Hadisiswoyo dan Bapak M. Yusuf Kartanegara, berfoto bersama Kepala Fasilitas Pemeliharaan dan Perbaikan (Fasharkan) Pangkalan TNI AL (Lantamal) V dalam kunjungan kerja ke Fasharkan Lantamal V Surabaya, Jawa Timur, Rabu, 21 Maret 2018.

4. Bapak Suharso Monoarfa, Anggota Wantimpres, melaksanakan kunjungan kerja ke Kantor Pusat Kfw (Bank Pembangunan di Jerman) di Frankfurt, Jerman, Senin, 26 Maret 2018. Dalam kegiatan tersebut, beliau berdiskusi dengan Dr. Christine Helmburger, *Director for East Asia and Pacific Kfw*.
5. Bapak Sidarto Danusubroto, Anggota Wantimpres, menghadiri Haul XV Hadrostusy Syekh KH Mahfudz Syafi'i dan Nyai Hj. Muchsonah yang diselenggarakan di Pondok Pesantren Al-Istighotsah, Bekasi, Jawa Barat, Sabtu, 31 Maret 2018.
6. Bapak Agum Gumelar, Anggota Wantimpres, membuka Diskusi Terbatas dengan tema "Upaya Mewujudkan Indonesia Menjadi Negara Maritim Ditinjau dari Aspek Hukum", di Wisma Elang Laut, Jakarta, Rabu, 4 April 2018.



7



8



9



10



11



12

- 7. Ibu Sri Adiningsih, Ketua Wantimpres, dan Bapak Sidarto Danusubroto, Anggota Wantimpres, melaksanakan pertemuan terkait uji kompetensi sertifikasi dan kelulusan mahasiswa kedokteran, di Kantor Wantimpres, Senin, 9 April 2018. Dalam pertemuan yang dihadiri perwakilan mahasiswa kedokteran tersebut, dibahas beberapa permasalahan yang timbul dari pelaksanaan Uji Kompetensi Mahasiswa Program Profesi Dokter (UKMPPD).
- 8. Bapak A. Malik Fajar, Anggota Wantimpres, disambut oleh para guru SMK Muhammadiyah Kabupaten Lumajang, Jawa Timur, Kamis, 12 April 2018. Kegiatan ini merupakan salah satu mata acara dari rangkaian kunjungan kerja beliau ke Kabupaten Lumajang guna meninjau perkembangan pendidikan, keagamaan, dan kesejahteraan rakyat di daerah dimaksud.
- 9. Ibu Sri Adiningsih, Ketua Wantimpres, menjadi narasumber dalam acara *1st Annual Economic Freedom Summit* yang diselenggarakan oleh *European Parliament* terkait *Past, Present and Future Market Reforms in Indonesia*, di *European Parliament*, Brussels, Belgia, Kamis, 12 April 2018. Beliau memberikan gambaran secara langsung mengenai perkembangan ekonomi dan pembangunan Indonesia, seperti perdagangan dan pertumbuhan ekonomi baru yang selaras dengan agenda Nawa Cita.

- 10. Bapak M. Yusuf Kartanegara, Anggota Wantimpres, menyelenggarakan Pertemuan Terbatas dengan tema "Perkembangan Teknologi Digital dan Dampaknya di Indonesia dalam Bidang Pertahanan dan Keamanan", di Kantor Wantimpres, Senin, 16 April 2018. Dalam kegiatan tersebut, hadir pula Ibu Sri Adiningsih, Ketua Wantimpres, dan Bapak Sidarto Danusubroto, Anggota Wantimpres, serta para narasumber dari berbagai kalangan.
- 11. Bapak Jan Darmadi, Anggota Wantimpres, menerima kenang-kenangan dari Bapak Jamartin Sihite, CEO *Borneo Orangutan Survival Foundation* (BOSF), selepas melaksanakan pertemuan di Kantor Wantimpres, Selasa, 17 April 2018. Dalam pertemuan tersebut, Bapak Jan Darmadi menerima aspirasi dari perwakilan BOSF mengenai strategi dan upaya pelestarian orangutan di Indonesia.
- 12. Bapak M. Yusuf Kartanegara, Anggota Wantimpres, berfoto bersama dengan peserta Rapat Tim Kajian di Kantor Wantimpres, Senin, 14 Mei 2018. Dalam kegiatan yang membahas tema "Optimalisasi Penanggulangan Penyalahgunaan Narkoba untuk Mewujudkan Keamanan yang Kondusif" tersebut, hadir sebagai narasumber, yakni Kepala Badan Narkotika Nasional (BNN), Deputi IV Badan Intelijen Negara (BIN), dan Bapak Asep Iriawan.

# WARTA Edisi 2 2018

