Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional

Kolonel Inf Sugeng Santoso, S.I.P.
Tenaga Ahli Pengkaji Muda Bidang Ideologi Lemhannas RI, Alumni PPRA LVI Lemhannas RI

ABSTRAK

Dalam perkembangannya perkembangan teknologi dapat membantu mempermudah aktivitas manusia, namun di sisi lain mengandung ancaman terhadap serangan siber. Serangan siber tersebut akan sangat mengancam keamanan negara, selain mengancam terhadap individu-individu juga dapat mengancam dengan skala yang lebih besar seperti fasilitas umum. Indonesia, sebagai negara pengguna internet terbesar, tidak terlepas dari ancaman ini. Dalam tulisan ini dibahas bagaimana memperkuat pertahanan siber dalam rangka meningkatkan ketahanan nasional.

PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi membawa berbagai implikasi kompleks dalam kehidupan manusia dan hubungan antar negara. Semenjak dikenalnya pola komunikasi melalui dunia maya atau internet, batas-batas konvensional yang dahulu dianut dan dipatuhi oleh konsensus internasional menjadi semu. Memasuki tahun 2017 penetrasi internet di seluruh dunia mencapai 50 persen dengan penduduk mencapai 7,4 miliar diikuti oleh pemakai internet lebih dari 3,7 miliar orang[1]. Kondisi ini disebabkan oleh semakin pesatnya kemajuan teknologi informasi yang salah satunya diikuti dengan semakin mudahnya orang menggunakan internet. Tingginya pemakai internet di seluruh dunia memang tidak bisa dihindari, akibatnya dunia semakin menjadi kecil, komunikasi antar individu dan antar negara menjadi lebih mudah dilakukan. Masyarakat dunia termasuk Indonesia telah banyak menghabiskan waktunya di dunia maya, atau wilayah siber *(cyberspace).* Dalam perkembangannya perkembangan teknologi dapat membantu mempermudah aktivitas manusia, namun di sisi lain mengandung ancaman terhadap serangan siber. Serangan siber dapat dilakukan oleh perorang atau negara, seperti kita ketahui ketergantungan terhadap internet sudah menjadi kebutuhan utama setiap pengguna teknologi dalam kehidupan sehari-hari, bahkan kantor pemerintah, swasta serta fasilitas pelayanan umum sangat tergantung terhadap penggunaan internet, sementara serangan siber makin kencang belakangan ini.

Data dari sejumlah lembaga memperlihatkan, aktivitas serangan meningkat. Beberapa kalangan

mengingatkan bahwa serangan siber juga mulai beralih dari mendapatkan keuntungan ekonomi ke kepentingan politik. Karena itu, pengamanan akses dan data perlu ditingkatkan. Kementerian Komunikasi dan Informatika (Kominfo) menyebutkan, serangan yang berdampak pada 10 juta lebih identitas terus meningkat. Tahun 2014, serangan berdampak pada 11 juta identitas, 2015 naik menjadi 13 juta identitas, dan 2016 naik lagi menjadi 15 juta identitas. Kominfo bahkan menyatakan, Indonesia merupakan salah satu dari 10 besar negara-negara di dunia yang masuk dalam target perang siber. Dari 10 negara sasaran, Indonesia berada di urutan kelima atau keenam. *Symantec,* sebuah perusahaan perangkat lunak, dalam *Internet Security Threat Report* tahun ini melaporkan serangan terhadap jaringan internet secara global. Semula, Indonesia berada di peringkat ke-29 pada 2015. Namun, tahun 2016, Indonesia menduduki peringkat ke-17. Surat elektronik *(e-mail)* dengan kandungan perangkat lunak perusak dari semula 1 dalam 236 surel kini menjadi 1 dalam 156 surel. Laporan *Akamai State of the Internet Security* pada triwulan pertama 2017 menyebut, Indonesia menempati peringkat ke-17 dalam serangan melalui 3,2 juta permintaan laman berbahaya terhadap pelanggannya. Para penyerang melihat data penggunaan internet yang mengindikasikan adanya perputaran uang dalam jumlah besar di negara itu sehingga mereka akan melakukan berbagai cara untuk mendapatkan keuntungan. Meski demikian, lembaga ini mengingatkan bahwa motivasi penyerang sekarang mulai beralih dari ekonomi ke kepentingan politik dengan melakukan sabotase, seperti di beberapa negara Timur Tengah. Indonesia cukup rentan karena masuk dalam 10 besar serangan siber[2]. Serangan siber tersebut akan sangat mengancam keamanan negara, selain mengancam terhadap individu-individu juga dapat mengancam dengan skala yang lebih besar seperti fasilitas umum seperti Rumah Sakit, Perbankan, Pembangkit Listrik, PDAM yang dampaknya akan merugikan individu-individu dan membahayakan situasi keamanan secara nasional dan pada akhirnya akan menggoyahkan ketahanan nasional.

PEMBAHASAN

Saat ini, penyalahgunaan jaringan internet di Indonesia sudah mencapai tingkat yang memprihatinkan. Maraknya kejahatan di dunia maya *(cyber crime)* merupakan imbas dari kehadiran teknologi informasi (TI), yang di satu sisi diakui telah memberikan kemudahan-kemudahan kepada manusia. Namun demikian, di sisi lainnya, kemudahan tersebut justru sering dijadikan sebagai alat untuk melakukan kejahatan di dunia maya *(cyber crime)* seperti yang sering kita saksikan belakangan ini. Risiko serangan siber kian meningkat baik pada masyarakat secara individu ataupun organisasi atau lembaga pemerintah yang makin bergantung pada teknologi dan internet. Apabila dilihat dari tujuan maka serangan atau ancaman siber dapat dibedakan menjadi beberapa hal sebagai berikut.

a. *Hactivism.*

Merupakan serangan siber yang bertujuan protes dan bermotifkan agenda politik atau sosial seperti kebebasan informasi, kebebasan berpendapat, hak asasi manusia atau anti kolonialisme, kelompok peretasnya

disebut hactivist. Salah satu group yang terkenal adalah anonymous. Seperti serangan Titan Rain 2005 yang menyerang industri pertahanan Amerika Serikat.

b. Krimninal.

Serangan siber yang satu ini memiliki tujuan kejahatan, bisa kejahatan ekonomi, untuk kejahatan ekonomi yang bermotif biasa contohnya memperoleh akses ke situs keuangan untuk memperoleh data yang bisa dijadikan kejahatan keuangan ataupun bisa mencuri data untuk dijual ke pihak ketiga seperti pembobolan *Yahoo* di Tahun 2013, bisa juga untuk tujuan mengambil data untuk memeras seperti kasus *WannaCry* di tahun 2017, pemerasan dilakukan lewat penguncian data dengan *enkripsi.* Di Indonesia contoh kejahatan siber yang mengemuka misalnya terjadi pada November 2016, ketika seorang remaja meretas akun situs tiket.com illegal access ini membuat pihak tiket. com mengalami kerugian sebesar 4.124.000.982 rupiah.

c. Perang siber.

Adalah serangan siber secara masif yang dilakukan oleh suatu negara atau penduduk suatu negara terhadap integritas siber negara lain dengan motif politik, seperti yang terjadi pada Estonia tahun 2007 dan di Iran yaitu *Stuxnet* terhadap reaktor nuklir Iran tahun 2010.

d. Spionase.

Serangan siber yang satu ini bertujuan memantau informasi dan mencuri data secara kontinu dari target sasaran. Spionasi ini bisa dilakukan oleh negara, pemerintah atau korporasi.

Oleh karena itu, untuk mencegah merajalelanya *cyber crime,* maka perlu dibuat aturan hukum yang jelas untuk melindungi masyarakat dari kejahatan dunia maya. Bahkan, dengan pertimbangan bahwa pengembangan teknologi informasi dapat menimbulkan bentuk-bentuk kejahatan baru, terutama dalam penyalahgunaan teknologi informasi, akhirnya pada 4 Desember 2001 yang lalu, PBB (Perserikatan Bangsa-Bangsa) mengeluarkan resolusi Nomor 55/63, dalam resolusi tersebut disepakati bahwa semua negara harus bekerja sama untuk mengantisipasi dan memerangi kejahatan yang menyalahgunakan teknologi informasi. Salah satu butir penting resolusi menyebutkan, setiap negara harus memiliki undang-undang atau peraturan hukum yang mampu untuk mengeliminir kejahatan tersebut.

Untuk menghadapi kejahatan siber tersebut maka harus ada upaya preventif melalui kebijakan dan kelembagaan, pemerintah sebagai pemangku kepentingan utama dalam pertahanan siber harus menyusun kebijakan yang menjalin semua pemangku kepentingan lainnya untuk melakukan prinsip dan implementasi keamanan dan ketahanan siber, hal tersebut harus dilakukan melalui peraturan perundang-undangan. Dari sisi kebijakan pemerintah telah mengeluarkan regulasi yang mengatur beberapa aspek penyelenggaraan dan keamanan siber seperti UU on. 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), UU No. 36/1999 tentang Telekomunikasi, dan UU Nomor 32/2002 tentang penyiaran namun semua UU tersebut hanya mengatur dari aspek keamanan dan

dan pertahanan siber, untuk lebih mengefektifkan upaya preventif harus ada UU yang mengatur kewenangan institusi negara yang berhak melakukan pengawasan terhadap penyelenggaraan sistem teknologi informasi baik institusi maupun korporasi.

Dari aspek kelembagaan Indonesia sebenarnya telah memiliki beberapa lembaga yang bertanggung jawab atas keamanan siber seperti Direktorat *Cyber Crime* pada Badan Reserse dan Kriminal (Bareskrim) Mabes Polri yang bertanggung jawab atas penyidikan kejahatan siber. Di samping itu pada tanggal 4 Mei 2007 diterbitkan Peraturan Menteri Nomor 26/PER/M. KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Menteri Komunikasi dan Informatika dalam hal ini menunjuk Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC)* yang bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet, Pemerintah juga telah membentuk Badan Siber dan Sandi Negara (BSSN) sesuai dengan Peraturan Presiden Nomor 53 tahun 2017 yang ditandatangi oleh Presiden Joko Widodo pada 19 Mei 2017. BSSN merupakan lembaga pemerintah non-kementerian yang berada di bawah dan bertanggung jawab kepada Presiden, pembentukan BSSN sebagai penguatan dari Lembaga Sandi Negara yang ditambah dengan Direktorat Keamanan Informatika. Dalam Peraturan Presiden itu disebutkan bahwa BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.

Diharapkan dengan hadirnya lembaga-lembaga tersebut akan menghadirkan standar keamanan siber yang kuat di tanah air, dengan tugas dan wewenang yang semakin rigid dalam mengamankan wilayah siber sehingga dapat menangkal setiap ancaman kejahatan siber yang dapat merugikan baik individu-individu maupun lembaga dan korporasi, Indonesia sebagai negara dengan penduduk penduduk keempat di dunia diikuti dengan penetrasi internet terbesar di dunia maka kewaspadaan harus tetap dipelihara, dan tidak boleh hanya negara yang berposisi sebagai pembeli dan pemakai namun dapat sebagai pemain penting terutama di kawasan Asia Tenggara dalam urusan siber harus mempunyai pertahanan yang kuat, dengan penguasaan teknologi siber dan pertahanan terhadap serangan siber maka diharapkan akan mendukung dan memperkuat Ketahanan Nasional.

PENUTUP

Kesimpulan

Dalam era globalisasi sekarang ini, ancaman keamanan terhadap kedaulatan setiap negara tidak hanya bersifat ancaman militer yang bersifat fisik semata, melainkan telah meluas ke ancaman non-fisik yang bersifat nirmiliter, yakni ancaman dunia maya atau ancaman siber, yang mengarah pada *cyber crime,* dan berpotensi menyebabkan *cyber warfare.* ancaman *cyber warfare* bersifat halus, tidak terlihat, dan sulit dirasakan, namun dampaknya sangat dahsyat, sehingga sangat membahayakan kemanan

suatu negara. Ancaman *cyber warfare* menyadarkan setiap negara di dunia, termasuk Indonesia untuk membentuk pertahanan siber, karena ancaman *cyber warfare* tidak bisa dihadapi dengan jumlah persenjataan, alutsista dan jumlah tentara yang banyak dan canggih, melainkan diperlukan regulasi serta SDM yang memahami teknologi informasi, komunikasi, komputer, internet, dan media sosial. Ancaman *cyber warfare* sudah saatnya mendorong Indonesia untuk menyusun ulang sistem pertahanan yang berbasis pada *cyber defence* dan *cyber security,* yang tentunya memerlukan persiapan yang matang dan sistematis dengan dukungan dari berbagai pihak. Sinergitas dalam menghadapi ancaman *Cyber Warfare* merupakan sebuah keniscayaan dan keharusan bagi Indonesia. Dengan sinergitas dan jalinan komunikasi, koordinasi, jaringan, dan kerja sama teknis harus dilakukan untuk membentuk komunitas pertahanan siber (*cyber Defence community)* yang dapat menangkal, mendeteksi, menangkis, dan mencegah secara dini berbagai potensi serangan ancaman cyber warfare sehingga dapat memperkokoh Ketahanan Nasional.

Saran

1) Pemerintah dalam hal ini Kementrian Pendidikan dan kebudayaan bekerjasama dengan Kemenristekdikti melakukan upaya terobosan untuk mendidik dan merekrut tenaga profesional keamanan IT yang memiliki integritas dan etika yang tidak tercela untuk medukung pengembangan dan menjalankan pertahanan siber.
2) Pemerintah bekerjasama dengan fihak investor membangun industri Teknologi Informasi nasional untuk mengembangkan perangkat keras dan lunak yang bisa digunakan untuk membangun pengamanan dan pertahanan siber nasional

---

DAFTAR PUSTAKA

Naskah Bahan ceramah Bidang Studi Lingstra kepada peserta PPRA LVI pada tanggal 27 Juli 2017 oleh Pratama Persada.

Materi Pokok Bidang Studi Lingkungan Strategis Lembaga Ketahanan Nasional 2017.

"Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy On The Facing Of Cyber Warfare Threat",Agus Subagyo Dosen FISIP UNJANI dan Seskoad Bandung subagyoeti@yahoo.com.au dan subagyo@scientist.com