ISSN: 22620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 1, No.2, 2018

Antisipasi Perang Siber: Postur Ketahanan Nasional Indonesia Merespon Ancaman Perang Siber

Muhammad Syaroni Rofii[4]

rony080@gmail.com

Abstract

These days cyber war is considered to be one of the important issues that have become the focus of defense officials of major countries. Cyber war has the same damage effect as traditional war even more massive. A country's nuclear installations can be destroyed with the help of cyber soldiers. The energy source of a country can also be disabled with the help of cyber troops. Or creating chaos in a country's election such as US election in 2016 also involving cyber troops. The same situation also happened in Indonesia whereby official website of general election commission, public companies and private companies were targeted by cyber attacks. Because of the attacks those institutions lost their data. Considering increasing number of cyber attacks, it is very necessary to learn form the US experience. This article attempt to investigate the trends in cyber war and the dynamics surrounding it. The paper also propose some reccomendation related to the national security of Indonesia in responding cyber threats either from state or non-state actors. **Keywords**: *cyberwar, national resilience, Indonesia*

Dewasa ini perang cyber dianggap sebagai salah satu masalah penting yang telah menjadi fokus para pejabat pertahanan negara-negara besar. Perang cyber memiliki efek kerusakan yang sama seperti perang tradisional bahkan lebih masif. Instalasi nuklir suatu negara dapat dihancurkan dengan bantuan tentara siber. Sumber energi suatu negara juga dapat dinonaktifkan dengan bantuan pasukan siber. Atau menciptakan kekacauan dalam pemilihan suatu negara seperti pemilihan AS pada tahun 2016 juga melibatkan pasukan siber. Situasi yang sama juga terjadi di Indonesia di mana situs web resmi komisi pemilihan umum, perusahaan publik dan perusahaan swasta menjadi sasaran serangan cyber. Karena serangan lembaga-lembaga itu kehilangan data mereka. Mengingat semakin banyaknya serangan cyber, sangat penting untuk belajar dari pengalaman AS. Artikel ini mencoba menyelidiki tren dalam perang cyber dan dinamika di sekitarnya. Makalah ini juga mengusulkan beberapa rekomendasi yang berkaitan dengan keamanan nasional Indonesia dalam menanggapi ancaman dunia maya baik dari aktor negara atau non-negara. **Kata kunci**: c*yberwar, ketahanan nasional, Indonesia*

[4] Dosen Kajian Stratejik Ketahanan Nasional, SKSG Universitas Indonesia

1. Pendahuluan

Perang siber atau ''cyber warfare'' adalah terminology baru yang muncul dalam kamus militer dan pertemuan-pertemuan para pejabat pertahanan dalam satu dekade terakhir. Perang *cyber* atau siber sangat berbeda dengan perang konvensional yang melibatkan senjata berat beserta personil militer dari berbagai kesatuan. Kendati sumber daya yang dikeluarkan sangat minim namun dampak kerusakan yang ditimbulkan oleh perang siber tidak jauh berbeda dengan perang konvensional. Dalam perang konvensional instalasi nuklir sebuah negara dihancurkan dengan menggunakan jet tempur, namun dalam perang siber cukup dengan membobol sistem radar dan sistem informasi militer sebuah negara maka instalasi nuklir bisa dirusak, diperlambat atau diledakkan. Iran termasuk negara yang pernah menjadi korban serangan siber yang mentargetkan instalasi nuklir mereka (abc.net.au, 20/02/19). Intervensi pihak luar dalam pemilu Amerika Serikat melalui serangan interet atau *cyber attack* juga menjadi sebuah fenomena baru dalam hubungan antar negara
(atlanticcouncil.org, 25/07/2017). Mengingat efektifitas serangan siber, Isac Ben Israel, seorang penasehat pertahanan pemerintah Israel dalam urusan perang siber menyebutkan betapa teknologi siber memiliki dampak kerusakan yang massif yang setara dengan serangan rudal, tanpa harus mengeluarkan sebutir peluru, sebuah negara mampu merusak sumber energy dengan bantuan serangan siber, "A cyber-war can inflict the same type of damage as a conventional war. If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting a single bullet" (Jeff Moss, 2012).

Selain perang siber menyasar instalasi militer, perang siber juga bisa menyerang sektor-sektor yang berkaitan dengan urusan warga sipil, seperti jaringan internet, sambungan telepon, rekening bank, kartu kredit hingga instalasi energy yang tersambung dengan jaringan computer dan internet. Untuk kasus Indonesia, kita bisa menjadikan pengalaman situs Komisi Pemilihan Umum, Bank Indonesia dan beberapa perusahaan swasta Indonesia yang sempat mengalami kehilangan data lantaran aksi serangan siber yang dilakukan oleh peretas (sindonews.com, 20/02/19).

Dari beberapa peristiwa di atas bisa ditarik sebuah kesimpulan, bahwa perang siber bukan ilusi, perang siber sedang terjadi namun tidak banyak yang menyadari keberadaannya. Menyadari keberadaan perang siber, maka negara-negara besar seperti Amerika, Inggris, Rusia dan China telah mengambil langkahlangkah strategis untuk mengantisipasi potensi serangan yang dilakukan oleh aktor negara dan aktor non-negara, baik dari dalam maupun luar negeri. Negara-negara besar tersebut telah membentengi diri untuk menghalau setiap serangan yang setiap saat mengintai sistem informasi mereka.

Dari paparan fakta di atas lantas muncul sejumlah pertanyaan meliputi, bagaimana awal mula perang siber di dunia? Seperti apa perkembangan tren perang siber dalam satu dekade terakhir? Bagaimana Indonesia mengantisipasi kemunculan perang siber ditengah meningkatnya konektivitas masyarakat Indonesia dengan dunia informasi?

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode kualitatif. Metode kualitatif menurut Earl R. Babbie (2013), adalah sebuah metode yang menekankan pada pengambilan kesimpulan berdasarkan observasi,

analisis wacana, interview mendalam atau teknik-teknik riset lainnya untuk mendapat kesimpulan non-numerik. Dalam melakukan penelitian ini penulis berupaya mengumpulkan data-data baik data primer maupun sekunder terkait perang siber yang terjadi di level nasional dan internasional untuk kemudian dilakukan analisa mendalam hingga mendapatkan kesimpulan seperti tertuang dalam penelitian ini.

Data primer yang dimaksud adalah berita-berita seputar serangan siber yang dilakukan oleh negara terhadap negara lain atau korporasi yang dipublikasikan oleh media-media mainstream dan memiliki dampak signifikan terhadap keamanan sebuah negara. Selain itu peneliti juga melakukan analisa terhadap situs-situs serta video terkait serangan siber terhadap objek-objek yang selama ini menjadi target serangan para *hacker* baik yang dilakukan oleh aktor negara maupun aktor non-negara. Sementara data sekunder yang dimaksud adalah paparan data yang disampaikan oleh para peneliti yang konsen dengan isu perang siber.

3. Definisi Perang Siber dan Trendnya

Sebelum mengelaborasi lebih jauh tentang perang siber sangat penting untuk memahami definisi yang umum digunakan oleh para peneliti dan pakar siber dalam menjelaskan fenonema perang siber. Paul Robinson, salah seorang peneliti perang siber misalnya memiliki definisi menarik tentang perang siber yang belakangan menjadi perhatian banyak pemimpin negara tersebut, dalam bukunya Robinson menekankan bahwa perang siber sangat menekankan pada penggunaan media computer dan internet baik untuk tujuan menyerang atau untuk bertahan. Kadang-kadang terminology perang siber juga dikaitkan dengan aktifitas operasi militer yang menggunakan teknik-teknik teknologi informasi. Sebab negara modern dan militernya telah memiliki ketergantungan pada computer. Serangan-serangan terhadap jaringan computer militer memiliki dampak kerusakan yang sama dengan serangan militer tradisional.

Perang Siber memiliki sejumlah tujuan: melakukan eksploitasi terhadap data informasi pihak lain atau berupa spionase; melakukan pengecohan terhadap musuh; melakukan pelacakan terhadap sistem informasi musuh atau mencegah musuh menggunakan sistem informasi milik mereka sendiri; dan pada akhirnya pihak musuh akan berupaya menghancurkan sistem informasi lawannya.

Sementara metode yang sering digunakan oleh negara-negara dalam menyerang targetnya, meliputi seranganserangan terhadap data, berupa spamming (sampah) yang dapat menyebabkan computer terganggu dan mengalami error; melakukan pembobolan terhadap computer negara lain dengan tujuan untuk mencuri informasi; serangan berupa software, berupa virus, worm dan bom logic hingga serangan fisik terhadap computer yang terhubung ke sistem milik negara (Paul Robinson, Dictionary of International Security (New York: Polity Press, 2007, 58).

Dari penjelasan Robinson kita bisa melakukan pemetaan terkait metode serangan para penyerang baik dilakukan oleh negara maupun non-negara dalam menjalankan aksinya. Jika melihat kasus Indonesia serangan terhadap situs Komisi Pemilihan Umum pada tahun 2014 dalam bentuk penggantian logo partai politik peserta pemilu dengan tujuan untuk menguji ketahanan situ KPU atau serangan terhadap situs Bank Indonesia oleh hacker luar negeri memperlihatkan bahwa target para peretas adalah institusi negara. Dampak kerusakan yang ditimbulkan sangat berbahaya bagi kelangsungan pemilihan umum Indonesia yang sedang berlangsung atau peretasan terhadap Bank Indonesia berpotensi membobol

data-data keuangan Indonesia dan seluruh nasabah.

Awalnya ancaman siber dilihat sebagai fenomena biasa yang melibatkan para hacker yang berupaya meraih keuntungan finansial dari aksinya yang menyasar pengguna individu atau perusahaan. Namun belakangan, negara terlibat langsung dalam perang siber, negara merespon perkembangan perang siber dengan menciptakan sistem untuk bertahan atau untuk menyerang. Amerika Serikat, Inggris, Israel, Rusia, China, Korea Utara, dan Iran merupakan negara-negara yang banyak disebut terlibat dalam perang siber, baik sebagai korban serangan atau sebagai pihak yang diduga melakukan serangan.

4. Perkembangan Wacana Perang Siber

Kendati wacana perang siber sering disampaikan oleh para pejabat pertahanan dalam forum-forum aliansi pertahanan NATO, pemerintah Amerika Serikat sendiri mengakui bahwa perang siber belum akan terjadi dalam waktu dekat akan tetapi dampak kerusakan yang diciptakan oleh perang siber sangatlah nyata. Richard A. Clarke selaku penasehat keamanan Gedung Putih dalam sebuah wawancara dengan *Journal of International Affairs* menjelaskan bahwa perang siber menyasar sektor-sektor yang terhubung dengan jaringan internet atau disebut dengan istilah ''Internet of Things'', contoh instalasi yang sering menjadi sasaran serangan adalah instalasi publik seperti reaktor nuklir yang terhubung dengan sistem internet, mesinmesin yang mendeteksi kelangsungan hidup pasien yang terhubung dengan sistem informasi, pipa saluran gas yang juga dikontrol melalui komputer. Contoh-contoh tersebut merupakan target sararan para penyerang, baik dilakukan oleh aktor negara maupun aktor non-negara (Richard A Clarke, 2016).

Namun demikian, pernyataan yang disampaikan oleh Clarke selaku penasehat pertahanan AS bisa dilihat sebagai upaya pengalihan isu mengacu pada kenyataan di lapangan terkait keterlibatan AS yang disebutsebut terlibat dalam pembuatan virus Stuxnet yang merupakan senjata berupa virus computer pertama yang mampu melumpuhkan instalasi nuklir Iran. Stuxnet sendiri disebut sebagai virus computer yang diciptakan oleh AS yang kemudian dikembangkan oleh Israel sehingga membuat virus Stuxnet sangat agressif dalam menyerang targetnya **(abc.net.au, 20/02/19).**

Harus diakuai bahwa AS, Israel, Inggris, China, Rusia, Iran, Suriah, dan Korea Utara merupakan negara-negara yang memiliki kemampuan untuk menyerang dan bertahan secara mumpuni dalam perang siber. Masingmasing negara memiliki detasemen khusus untuk mengurus urusan serangan siber dengan sebutan berbeda-beda.

Jika menggunakan contoh AS, AS memiliki sejarah panjang dalam urusan pengembangan pasukan yang bekerja khusus untuk menyerang dan menangkal serangan siber. Kendati setiap presiden AS memiliki kharakteristik sendiri dan memiliki kebijakan yang berbeda-beda dalam urusan perang siber namun mereka memiliki fundamen yang kuat dalam merancang bangunan pertahanan nasional mereka. Jika selama Perang Dingin hingga Tragedi Serangan Bom Menara Kembar 2001, presiden-presiden AS memberikan keleluasaan bagi badan-badan yang bergerak di dibidang pertahanan dan infomrasi intelelijen. Ronald Reagan dikenal sebagai presiden AS yang memiliki konsen sangat tinggi terkait isu serangan non tradisional dari musuh-musuh AS dengan mengeluarkan dekrit National Security Decision Directive-145 atau NSDD-145 yang berjudul "National Policy on Telecommunications and Automated

Information Systems Security"(Fred Kaplan, 2016).

Keluarnya dekrit tersebut ditujukan untuk mengantisipasi serangan yang tidak secanggih serangan rudal lintas benua namun memiliki dampak kerusakan yang sama bagi keamanan nasional. Presiden AS lainnya George W. Bush juga memanfaatkan perkembangan teknologi informasi untuk mensukseskan operasi militer Perang Irak 2003. Selanjutnya, Presiden Barack Obama, kendati tidak memberikan keleluasaan secara luas kepada badan intelijen untuk mengakses informasi dan melakukan pengintaian kepada warga AS karena pertimbangan kebebasan sipil namun dibelakang layar, melalui menteri Pertahanan Robert Gates, AS membentuk Cyber Comand (Pusat Komando Siber) yang mendapat alokasi anggaran cukup tinggi. Pada tiga tahun pertama badan ini mendapat anggaran dari angka 2.7 milyar dollar menjadi 7 milyar dollar (ditambah dengan 7 milyar dollar lainnya untuk aktifitas siber di lingkungan militer. Sementara jumlah pasukan siber AS dari tahun ke tahun mengalami peningkatan, mulai dari 900 personil kemudian menjadi 4000 personil, data terakhir seperti disebutkan Fred Kaplan dalam bukunya, mencapai 14.000 personil (Kaplan, 2016).

AS sendiri belakangan banyak menggunakan metode non-konvensional untuk menaklukkan target-targetnya, NSA dan CIA sebagai badan intelijen diberi peran lebih besar untuk melakukan operasi di Irak. Sejak tahun 2007 misalnya, AS lebih banyak mengirim operator-operator yang memahami sistem komputer dan intelijen, sementara pasukanpasukan organik ditarik karena menganggap penggunaan instrumen perang siber lebih efektif. Sejak tahun 2007 AS yang saat itu kendali operasi dipegang oleh David Petraeus juga membuka kantor perwakilan di Irak di Al Balad Air Base. Dengan operasi yang memaksimalkan peran teknologi informasi, AS berhasil melumpuhkan empat ribu pemberontak Irak. Penumpasan pemberontak sangat terbantu oleh sistem yang dikenal dalam kamus operasi militer AS sebagai RTRG (Real Time Regional Gateway) atau Saluran Langsung Komunikasi Regional
(Kaplan, 2016).

Kasus lain yang menunjukkan peran teknologi informasi dalam operasi intelijen adalah saat Israel melakukan operasi yang disebut dengan Orchard Operation, dalam operasi ini jet tempur militer Israel F-16 melakukan penyerangan terhadapa instalasi nuklir Syria yang berhasil dibangun oleh ilmuan asal Korea Utara, jet tempur militer Israel berhasil meledakkan instalasi nuklir Syria tanpa diketahui oleh penjaga radar, dibalik serangan tersebut terdapat peran Unit 8200 Israel yang berhasil membobol sistem radar militer Syria dengan program yang dikenal dengan Suter. Unit 8200 diketahui memiliki jejak sukses dalam operasi-operasi intelijen (Kaplan, 2016).

Begitu juga dengan pola serangan siber yang dialami oleh Estonia juga sangat menarik untuk menegaskan tentang adanya perang siber yang melibatkan negara. Pada bulan April tahun 2007 Estonia merupakan korban dari serangan siber yang diduga datang dari Rusia. Serangan siber berawal dari ketegangan yang dipicu oleh sentimen anti-Rusia yang disampaikan oleh Presiden Estonia yang mengeluarkan kebijakan hendak menghilangkan patung-patung perunggu yang berdiri di kota Talin. Sebagian kelompok di Estonia melakukan protes yang diekenal dengan Bronze Night dan melakukan perusakan terhadap patung monumen Rusia, polisi berupaya mengamankan patung-patung yang ada di kota agar tidak terus menerus menjadi sasaran kebencian yang juga memicu bentrokan etnis. Tidak lama berselang Estonia mendapat serangan siber secara bertubi-tubi yang menyasar jaringan internet dan telepon. Warga

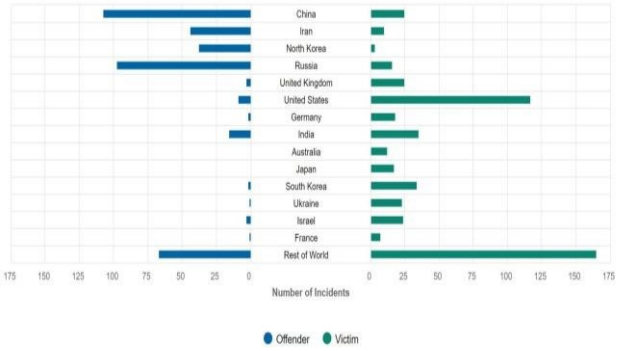
Estonia sempat mengalami kesulitan karena selama tiga minggu tidak mampu menggunakan jaringan telepon, rekening bank, kartu kredit, selain itu jaringan yang terhubung dengan parlemen, kementrian, kantor pemerintah, toko-toko, komunikasi militer mengalami gangguan (Kaplan, 2016).

5. Potret Perang Siber Kontemporer

Pada tahun 2013 sebuah laporan yang dirilis oleh Departemen Pertahanan Amerika Serikat yang disampaikan kepada kongres mengenai masalah China menyebutkan bahwa pemerintah China melalui Tentara Pembebasan Rakyat (People Liberation Army) memiliki divisi khusus yang bertujuan untuk melakukan serangan terhadap negara-negara yang dianggap "musuh", divisi tersebut merefleksikan perubahan visi pertahanan China dengan menjadikan ancaman dunia maya sebagai salah satu masalah penting yang harus direspon. Oleh sebab itu China mendirikan institusi khusus untuk melakukan respon terukur untuk masalah ini. Bahkan Cina memiliki terminologi sendiri untuk menjelaskan misi mereka di dunia cyber, Cina misalnya, menggunakan terminologi Perang Elektronik (EW) untuk menjelaskan posisi mereka di panggung dunia dan keamanan dunia maya (United States Department of Defense, Annual Report to Congress, Military Security and Development, Involving the
People's Republic of China 2013, 37).

NATO dalam dokumen yang mereka rilis pada tahun 2012 menyebutkan langkahlangkah antisipasi yang bisa diambil oleh pemerintah dalam rangka merespon perkembangan keamanan di dunia maya (cyber security), meliputi: Military Cyber (Tentara Siber), bahwa sejak tahun 2007 perusahaan McAfee telah memperingatkan bahwa perang senjata virtual sedang terjadi ditandai dengan peluncuran senjata siber oleh sejumlah negara; Counter Cyber
Crime/Menangkal Kejahatan Siber, aktifitas kejahatan dunia maya dapat membahayakan individu dan negara seperti pencurian data individu atau perusahaan berupa pencurian hak kekayaan intelektual; Intelligence and Counter Intelligence (Intelijen dan Kontra Intelijen), pola pengintaian yang dilakukan mata-mata yang dilakukan oleh militer negara-negara; Perlindungan Infrastruktur Vital dan Manajemen Krisis Nasional, perlindungan infrastruktur vital merupakan sarana penting dalam skema keamanan nasional sebuah negara; Cyber Diplomacy dan Internet Government (Diplomasi Dunia Maya dan Pemerintahan Internet) diplomasi dunia maya merupakan sebuha keniscayaan yang harus diterima, oleh sebab itu diplomasi modern merupakan bentuk adaptasi atas perubahan tata aturan dunia saat ini'' (Alexander Klimburg, ed, 2012).

Data yang dirilis oleh CSIS Amerika Serikat juga memperlihatkan intensitas serangan siber yang dilakukan oleh peretas yang bersumber dari negara-negara yang selama ini dianggap memiliki kemampuan siber handal. Sepanjang tahun 2018 hingga 2019 terlihat China, Iran, Korea Utara, Rusia, Inggris, dan Amerika Serikat masuk dalam kategori negara yang paling sering menjadi sasaran serangan dan diduga sebagai penyerang dalam insiden di dunia siber. Sementara sasaran serangan siber sebagian besar ditujukan kepada instansi pemerintah, mitra kerja pemerintah, perusahaan teknologi, serta perusahaan yang bergerak di sektor keuangan. Jumlah serangan yang terus meningkat menunjukkan adanya trend peningkatan keterlibatan negara dalam aktifitas serangan siber. Hal ini dipertegas oleh data berikut pada gambar 1.



Gambar 1. Insiden-insiden Penting Siber antara tahun 2016-2019

Sumber: CSIS & Hackmageddon

6. Respon Indonesia

Melihat sejumlah peristiwa-peristiwa penyerangan siber di Indonesia dalam sepuluh tahun terakhir, bisa dilihat bahwa Indonesia termasuk negara yang kerap menjadi korban serangan peretas, serangan siber sebagian besar menyasar situs-situs milik pemerintah serta lembaga yang menyangkut urusan banyak orang seperti Komisi Pemilihan Umum dan Bank Indonesia. Oleh sebab itu sangat penting bagi Indonesia melakukan antisipasi dini terhadap kemungkinan-kemungkinan serangan siber yang berpotensi melumpuhkan sumber-sumber energy serta pencurian data. Sebagai bentuk respon pemerintah atas dinamika internasional, pemerintah Indonesia juga sepertinya menyadari bahwa ancaman siber semakin nyata. Oleh sebab itu diciptakanlah sebuah regulasi untuk memaksimalkan pertahanan nasional di dunia maya dengan membentuk Badan Siber dan Sandi Negara selanjutnya disingkat BSSN melalui Peraturan Presiden Nomor 53 Tahun 2017. Di dalam peraturan presiden ini terlihat sangat jelas bahwa fungsi utama badan siber adalah untuk mengantisipasi segala bentuk serangan yang berpotensi mengancam stabilitas nasional dan ketahanan ekonomi nasional. Poin ini bisa dilihat pada pasal 3 peraturan tersebut yang menyebutkan bahwa BSSN bertugas untuk : ‘’..penyusunan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber’’.

Dilihat dari alasan pendirian dan tugastugas yang diberikan oleh BSSN, kita bisa melihat bahwa lembaga ini berdiri ditujukan untuk menjadi lembaga yang membentengi data Indonesia secara keseluruhan. Menjaga data-data Indonesia dari kemungkinan pencurian dan serangan dari luar. Selain itu lembaga baru ini memiliki fungsi koordinasi atas semua lembaga negara yang memiliki kaitan langsung dengan sistem informasi di Indonesia. Kendati pendirian BSSN tergolong terlambat namun paling tidak pemerintah Indonesia telah memahami peta ancaman kontemporer yang berpotensi mengancam ketahanan nasional Indonesia.

Bagi Indonesia yang saat ini tengah mempersiapkan penyelenggaran pemilihan umum tentu saja menjadi sebuah keniscayaan untuk melakukan deteksi dini atas setiap potensi serangan siber yang datang dari dalam maupun luar negeri baik yang dilakukan oleh aktor negara maupun non-negara. Instalasi yang sangat rawan menjadi sasaran serangan siber pada masa-masa sekarang adalah sistem informasi Komisi Pemilihan Umum (KPU), Badan Pengawas Pemilu, bank data Departemen Dalam Negeri, serta instansi pemerintah yang terkait langsung dengan urusan pemilu. Selain penyelenggara pemilu, para peserta pemilu juga berpotensi menjadi sasaran serangan, seperti partai politik, calon anggota legislatif, hingga calon presiden yang saat ini sedang terlibat

dalam kampanye hingga pemilihan pada bulan April 2019.

Terkait potensi serangan yang terjadi menjelang pemilu Indonesia perlu belajar dari pengalaman AS, AS kendati memiliki sistem pertahanan siber yang tangguh namun dalam kenyataanya serangan siber asing mampu menembus sistem keamanan panitia Konvensi Partai Demokrat yang kemudian menjadi isu nasional yang membuat hubungan AS dan Rusia memburuk. Serangan siber yang diduga dilakukan oleh kelompok hacker asal Rusia membuat citra Presiden AS saat itu Barack Obama memburuk karena dianggap tidak mampu membentengi keamanan nasional negaranya. Akibat serangan hacker tersebut AS mengeluarkan sanksi kepada diplomat Rusia (David P. Fidler, 2017).

Pelajaran lain yang bisa diambil dari pengalaman AS adalah adanya potensi penciptaan disinformasi atau penyesatan informasi. Seperti diakui Alexander Klimburg, salah seorang pakar keamanan siber yang juga penulis buku ‘’The Darkening Web: The War for Cyberspace’’, menyebutkan bahwa dalam peristiwa penyerangan peretas pada pemilu AS tahun 2016 penyesatan informasi memiliki kontribusi dalam penciptaan kekacauan di AS. Sebab menurut survey hanya 20 persen warga AS percaya pada media mainstream, sementara hanya 6 persen yang percaya pada Kongres AS, statistic ini menujukkan bahwa terdapat potensi untuk membombardir public AS dengan informasi yang bersumber dari sumber-sumber non-mainstream yang banyak diproduksi oleh para peretas (www.attlanticcouncil.org, 20/01/19) .

Oleh sebab itu Indonesia yang hendak menggelar pemilu pada tahun 2019 sangat perlu untuk memperhatikan keamanan data dan membentengi Indonesia agar mampu menghalau potensi serangan siber yang bertujuan untuk menyesatkan public dengan informasi yang keliru. Pada pemilu 2019 angka pemilih mencapai 192 juta dengan tingkat literasi digital yang rendah akan menjadi sasaran empuk bagi para penyerang untuk membombardir dengan informasiinformasi tidak besar berupa berita palsu dan isu-isu yang dibuat untuk menciptakan kekacauan dan berujung pada distabilitas nasional.

Selain terkait pemilu, sektor lain yang perlu menjadi objek yang perlu mendapat penjagaan oleh BSSN adalah sektor yang berkaitan dengan industry pertahanan, energy dan keuangan. Sebab sektor ini merupakan sektor yang selalu menjadi incaran para peretas. Perusahaan seperti PT Pindad, PT PAL, dan PT Dirgantara Indonesia adalah perusahaan yang mengandalkan kerahasiaan data untuk setiap produk mereka demi daya saing di tingkat internasional. Kehilangan data berarti kehilangan daya saing. Oleh sebab itu, penjagaan atas sektor strategis ini sangat penting dilakukan karena berkaitan langsung dengan kebutuhan nasional dan kepentingan nasional Indonesia.

7. Simpulan

Perkembangan teknologi saat ini mempermudah para penggunanya dalam setiap aktifitas. Dengan kemampuan teknologi para pelaku usaha dapat mempercepat produksi mereka, mempercepat distribusi, menghemat biaya dan keuntungan lainnya. Begitu juga ketika teknologi diadaptasi oleh negara untuk kepentingan pertahanan nasional. Sebuah negara yang mengadopsi teknologi pertahanan mutakhir sangat terbantu dengan kehadiran teknologi mutakhir. Sebut saja kehadiran teknologi drone yang mampu memetakan posisi musuh secara tepat dan real time atau teknologi satelit yang memudahkan para tentara yang bertugas di lapangan untuk mengetahui keberadaan musuh di medan

tempur yang sebelumnya tidak pernah mereka datangi.

Namun perkembangan teknologi informasi juga bisa menjadi sumber ancaman bagi negara, dalam hal ini serangan siber, keberadaan serangan siber semakin nyata untuk saat ini hal itu dibuktikan oleh data serangan sepanjang tahun 2018 dan tahun 2019 yang menunjukkan bahwa negara tidak diam, negara terlibat langsung dalam aktifitas serangan siber, oleh sebab itu Indonesia juga harus aktif dalam memetakan setiap potensi serangan demi keamanan dan ketahanan nasional Indonesia.

Kendati perang siber tidak begitu menjadi prioritas perhatian para pengambil kebijakan, namun demikian dampak dari perang siber sangat nyata dan menyentuh langsung kehidupan masyarakat. Serangan siber yang dikendalikan dibalik layar monitor mampu mematikan listrik sebuah kota, memutus saluran air, menciptakan kerusuhan, membobol data-data nasabah, hingga memicu destabilitas nasional adalah beberapa contoh dampak serangan siber.

Atas alasa tersebut maka tidak ada kata terlambat bagi pemerintah Indonesia untuk merespon perkembangan ancaman siber dengan melakukan pemetaan atas setiap potensi serangan serta melakukan perbaikan pada sistem informasi yang menyangkut data warga negara Indonesia. Selain itu pemerintah juga perlu memaksimalkan peran Badan Siber dan Sandi Negara untuk mengamankan setiap sektor yang berpotensi menjadi sasaran target para penyerang.

Daftar Pustaka

Babbie, Earl, The Practice of Social Research, Australia : Wadsworth Cengage Learning, 2013.

David P. Fidler ‘’The U.S. Election Hacks, Cybersecurity, and International Law’’ 2017, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3607&context=facpub.

Journal of International Affairs, Vol. 70, No. 1, The Cyber Issue (Winter 2016).

Kaplan, Fred, Dark Territory: Secret History of Cyber War, New York: Simon and Schuster, 2016.

Klimburg, Alexander, and Hugo Zylberberg, Cyber Security Capacity Building: Developing Access , NUPI Report, Report no. 6, 2015.

Moss, Jeff, et.all, “Cyber-security: The Vexed Question of Global Rules, An Independent Report on cyberpreparedness around the world”, Security Defense Agenda and McAfee Company, 2012.

Nye, Joseph S., The Regime Complex for Managing Global Cyber Activities, Belfer Center for Science and International Affairs, November 2014.

National Geographic, The Future of Cyberwarfare, in https://www.youtube.com/watch?v=L78r7YD-kNw, akses 20 February 2019.

Richard A. Clarke, The Risk of Cyber War And Cyber Terrorism,

Robinson, Paul, Dictionary of International Security, New York: Polity Press, 2007.

Stuxnet: The Real life Sci-fi Story of ‘’the world’s first digital weapon’’, www.abc.net.au, diakses 20/02/19.

The Risk of Cyber War And Cyber Terrorism Author(s): Richard A. Clarke

United States Department of Defense, Annual Report to Congress, Military Security and Development, Involving the People’s Republic of China 2013.

Wall, D. (2007) Cybercrime: The Transformation of Crime in the Information Age, Polity Press 2007.

Xiaojing Zeng, ‘’Multistakeholder Approach

Touted in Response to Cybersecurity Challenge'', www.atlanticcouncil.org, akses 20 Feb. 2019.