ISSN (e) : 2527–564X / ISSN (p) 2621-0746
Website Journal : http://www.ejournal-academia.org/index.php/renaissance

SIBER INTELIJEN UNTUK KEAMANAN NASIONAL

Dwi Rezki Sri Astarini[*)]; Muhammad Syaroni Rofii
Sekolah Kajian Strategik dan Global Universitas Indonesia
[*)]*email: dwi.rezki81@ui.ac.id*

Paper Accepted: 25 Februari 2021
Paper Reviewed: 26-31 Maret 2021
Paper Edited: 01-15 April 2021
Paper Approved: 25 April 2021

ABSTRAK

Penelitian ini membahas tentang siber intelijen untuk keamanan nasional. Suatu negara dituntut untuk dapat menguasai teknologi informasi dan komunikasi secara baik dan benar serta tepat guna, karena dunia siber dapat menjadi potensi ancaman serta penyelenggaraan keamanan siber yang belum terintegrasi dapat berdampak terhadap kedaulatan negara dan ketahanan nasional. Intelijen dijadikan alat untuk mendeteksi dini ancaman – ancaman siber yang datang dari dalam atau luar negeri. Penelitian ini termasuk dalam jenis penelitian desktriptif dengan menggunakan pendekatan kualitatif serta metode pengumpulan data melalui observasi, studi kepustakaan, wawancara dan dokumentasi. Penelitian ini bertujuan untuk: (1) Mengetahui kedudukan siber intelijen didalam bidang intelijen; (2) Siber intelijen dalam tata kelola intelijen negara. Hasil dari penelitian ini adalah peran siber intelijen sebagai bentuk "baru" dalam tata kelola intelijen negara dapat menjadi lebih jelas dan menghindari permasalahan yang mungkin dapat timbul. Dalam hal ini, perhatian terhadap isu-isu ini harus dibarengi dengan adanya solusi dalam menyiapkan sumber daya manusia, infrastruktur, dana dan teknologi yang mumpuni untuk dapat menjadikan siber intelijen sebagai aset bagi kepentingan keamanan nasional dan negara

Kata Kunci: Cyber, Intelligence, Information, National Security

PENDAHULUAN

Dalam era perkembangan teknologi dan informasi saat ini, ancaman terhadap keamanan juga menjadi semakin kompleks. Walaupun infrastruktur menjadi semakin canggih untuk mengakomodasi perubahan yang cepat, keberadaannya justru menempatkannya pada posisi yang kritikal. Graham (2010) menyatakan infrastruktur canggih yang dibangun di masa modern ini sebenarnya bersifat rentan karena menyimpan potensi kegagalan yang dapat berakibat fatal karena semakin tergantungnya manusia pada teknologi yang bertanggung jawab pada hajat hidup orang banyak. Dengan semakin terintegrasinya pusat-pusat data maupun infrastruktur penting baik yang bersifat fisik maupun non-fisik ke dalam jaringan teknologi dan global selain memberikan kemudahan akses dan kontrol juga menempatkannya pada risiko keamanan baru. Risiko ini di antaranya bersumber dari adanya ancaman intrusi yang dilancarkan dari dunia maya yang mampu menembus sistem jaringan keamanan data dan informasi terhadap pusat dan infrastruktur penting tersebut.

Pada tingkat negara, keberadaan ancaman dunia maya terhadap keamanan menjadi penting untuk diperhatikan. Pada saat ini, serangan/perang dunia maya (*cyber attack/cyber warfare*) dianggap sebagai media yang sangat ampuh untuk mengguncang stabilitas keamanan negara karena memiliki karakterstik yang murah, mudah dijalankan, dan efektif mencapai hasil yang diharapkan (Caplan, 2013). Sementara itu, upaya untuk menciptakan ketahanan terhadap serangan *cyber* tersebut lebih sulit untuk dilakukan disebabkan oleh adanya interkoneksi antara jaringan yang kompleks yang juga memberikan keleluasaan bagi aktor untuk bersembunyi dan melakukan serangan dari berbagai tempat di bumi ini.

Ancaman siber menjadi semakin luas dilihat dari segi teknik yang digunakan, sasaran yang

dituju, maupun dampak yang ditimbulkan, dengan demikian ada kemungkinan pada suatu saat negara akan mengalami kondisi yang tidak aman. Suatu negara berada dalam kondisi aman yaitu selama bangsa tersebut tidak dapat dipaksa untuk mengorbankan nilai-nilai yang dianggapnya penting (vital). Keamanan TIK merupakan permasalahan krusial yang harus diperjuangkan secara serius sebagai komponen pertahanan negara, karena masalah utama yang dihadapi setiap negara adalah membangun kekuatan untuk menangkal atau mengalahkan suatu serangan. Program peningkatan edukasi dan kesadaran keamanan siber disusun dengan target yang ditetapkan dengan baik, tetapi beberapa organisasi pemerintah melakukan program tanpa ada koordinasi yang terintegrasi dengan baik, seperti Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Ditkaminfo, Ditjen Aptika, Kominfo), Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), dan Lembaga Sandi Negara (Lemsaneg). Tidak ada portal daring pusat yang terhubung yang berguna untuk peningkatan kesadaran keamanan siber, kampanye kesadaran keamanan siber nasional yang terbatas dan materi yang tersedia untuk publik terkait keamanan siber masih sedikit.

Pada saat ini, sejumlah negara telah mengangkat isu *cyber security* ini sebagai suatu pokok bahasan dalam strategi keamanan nasional. Sebagai contoh, sejak peristiwa 9/11, pemerintah Amerika Serikat telah mengantisipasi ancaman dunia maya ini dengan mendirikan National Cyber Security Division (NCSD) di bawah Department of Homeland and Security (DHS) pada tahun 2003. Pada tahun 2015, Amerika Serikat dalam rilisnya terkait National Security Strategy juga menyerukan semakin perlunya meningkatkan kerja sama antar lembaga dalam rangka menciptakan ketahanan terhadap serangan dari dunia maya (Bisson, 2015). Perhatian yang sama juga semakin meningkat di negara-negara Eropa. Spanyol pada tahun 2013 telah mengeluarkan National Cyber Security Strategy untuk mengantisipasi ancaman *cyber* yang diperkirakan akan terus meningkat di masa mendatang.

Sementara itu, Inggris bahkan telah memiliki lembaga otoritas khusus untuk *cyber security*, yaitu The National Cyber Security Centre (NCSC). Namun demikian, fenomena ini belum menjadi fokus utama khususnya di negara-negara Asia kecuali Cina. Negara-negara di kawasan Asia merupakan target dari 80% serangan *cyber* dari berbagai dunia (BBC, 2016; Zheng, 2015). Pada saat yang sama walaupun Cina menjadi salah satu kekuatan besar di Asia dalam meningkatkan kemampuan *cyber security* maupun perannya dalam *cyber attack* namun hingga saat ini negara tersebut mengalami hambatan dan kendala yang bersumber dari masih lambat dan belum terkoordinasinya kebijakan yang menyeluruh terkait *cyber security* (Lindsay, 2015).

Indonesia merupakan salah satu negara yang menjadi anggota *Association of Southeast Asian Nations* (ASEAN) dihadapkan dengan kondisi perekonomian digital di kawasan regional ASEAN yang berpotensi meningkatkan nilai Produk Domestik Bruto (PDB) dalam beberapa tahun ke depan. Namun, ancaman siber dapat menghambat kepercayaan dan ketahanan ekonomi digital serta menghambat ASEAN untuk mewujudkan potensi digital secara optimal. Negara di kawasan ASEAN dimanfaatkan sebagai sasaran serangan siber dengan memanfaatkan titik rawan infrastruktur yang tidak aman. Relevansi ekonomi strategis yang berkembang di kawasan ini menjadikan ASEAN sebagai sasaran utama serangan siber, pada umumnya karena ketahanan siber dan tingkat kesiapan siber yang masih rendah. Secara khusus, tidak adanya pola pikir strategis, kesiagaan kebijakan, dan pengawasan kelembagaan yang berkaitan dengan keamanan siber. Selain itu, ancaman siber hanya dianggap sebagai masalah Teknologi Informasi dan Komunikasi daripada masalah bisnis, bisnis regional tidak memiliki pendekatan yang komprehensif dalam hal keamanan siber.

Tata kelola dan kebijakan keamanan siber belum dikembangkan di kawasan regional ASEAN. Strategi keamanan siber nasional telah ditetapkan oleh Singapura, Malaysia, Thailand, dan Filipina. Beberapa negara ASEAN telah membentuk badan nasional yang bertugas mengonsolidasikan dan mengkoordinasikan agenda keamanan siber yaitu termasuk Singapura (*Cyber Security Agency of Singapore*), Malaysia (*The National Cyber Security Agency*) dan Filipina (*Department of Information and Communications Technology*). Meskipun negara ASEAN lain tidak memiliki badan khusus, tetapi saat ini *Computer Emergency Response Teams* (CERT) atau *Computer Security Incident Response Teams* (CSIRT) memainkan peran lembaga keamanan siber di beberapa negara kawasan ASEAN.

Keamanan siber memiliki peran penting dalam menjaga keamanan informasi karena menjadi hal yang krusial untuk menjaga data dalam media penyimpanan dan menjamin informasi yang dikirim dalam keadaan aman serta perlindungan sistem informasi terhadap

ancaman siber. Peningkatan perlindungan terhadap informasi dan sistem terhadap akses yang tidak sah melalui kerahasiaan, integritas, ketersediaan informasi, nir-penyangkalan, dan otentikasi guna menghindari serangan siber. Termasuk menyediakan pemulihan sistem informasi dengan menggabungkan kemampuan mendeteksi, melindungi, dan merespon. Tata kelola keamanan siber di Indonesia masih bersifat parsial dan sektoral sehingga menyebabkan penanganan permasalahan keamanan siber belum terintegrasi dan belum terpadu. Hal tersebut menjadikan ancaman siber semakin nyata, terutama bila dikaitkan dengan ancaman ketahanan dan keamanan siber bagi pemerintah sebagai penyelenggara layanan publik sektor IIKN, pelaku ekonomi digital. Oleh karena itu, pengelolaan keamanan siber mutlak dilakukan secara terpadu untuk mencegah ancaman siber pada segala aspek kehidupan berbangsa dan bernegara. Terdapat beberapa organisasi pemerintah yang berurusan dengan komponen keamanan siber, seperti Kementerian Koordinator Bidang Politik, Hukum dan Keamanan (Kemenko Polhukam), Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Pertahanan (Kemhan), Badan Intelijen Negara (BIN), Tentara Nasional Indonesia (TNI), dan Kepolisian Republik Indonesia (POLRI), serta Lembaga Sandi Negara (Lemsaneg) yang bertransformasi menjadi BSSN. Namun, berbagai program terkait keamanan siber yang disusun dan dilaksanakan masih pada level masing-masing instansi pemerintah dan belum ada titik fokus (*focal point*) formal sebagai pemegang komando koordinasi dan pengembangan keamanan siber di Indonesia.

Tinjauan Teoritis

Teori Keamanan Nasional

Teori Keamanan Nasional adalah secara umum dan teori perang asimetris dan teori komunikasi akan digunakan dalam pembahasan yang lebih mendalam. Teori Keamanan Nasional menurut Alan Collins (2003) adalah "*National security is the requirement to maintain the survival of the nation-state through the use of economic, military and political power and the exercise of diplomacy.*"

Keamanan nasional adalah sebuah kebutuhan untuk menjaga ketahanan suatu bangsa melalui daya ekonomi, militer serta kekuatan politik dan kepiawaian berdiplomasi. Karena sifat yang kompetitif diantara bangsa-bangsa, keamanan nasional dengan negara yang mempunyai nilai sumber daya yang signifikan didasarkan kepada tindakantondakan teknis dan proses operasional. Hal ini berkisar dari perlindungan informasi yang berkaitan dengan rahasia Negara untuk persenjataan bagi militer hingga strategi bernegosiasi dengan negara bangsa lain. Oleh itu harus dilakukan beberapa langkah bagi memastikan keamanan negara terus dipelihara.

Teori Intelijen

Michael Warner (2006) Office of the Director of National Intelligence, dalam presentasinya mengenai Intelijen mengatakan bahwa Intelijen memiliki banyak makna bagi beberapa orang. Mengartikan Intelijen kedalam 1 (satu) definisi akan sangat sulit dilakukan, terdapat 2 (dua) definisi yang sering digunakan secara umum yaitu "Intelijen bagi Pengambil Keputusan" dan definisi lainnya "Intelijen adalah aktifitas rahasia suatu Negara untuk memahami dan mempengaruhi entitas asing". Mengutip pemikiran Sun Tzu (1963) , yang menambahkan istilah "Spionase" dalam Intelijen, yang merupakan penerjemahan atas informasi dan aksi, lebih lanjut terdapat doktrin yang dikatakan oleh Sun Tzu, Intelijen harus bekerja secara rahasia "Ketika agen tipe ini bekerja secara simultan dan tidak ada yang mengetahui metode operasi, mereka disebut "*The Devine Skein*" dan merupakan harta karun atas kedaulatan.

Hank Prunckun (2010), salah satu penulis tentang Intelijen dalam bukunya membuat 4 (empat) definisi dari Intelijen:

1. Tindakan
2. Tempat produksi pengetahuan
3. Organisasi yang menangani pengetahuan
4. Laporan yang dihasilkan dari proses ataupun organisasi

Hank Prunckun juga menjelaskan lebih mendalam 2 (dua) definisi lainnya mengenai Intelijen, yaitu sebagai pengetahuan dan sebagai proses.

- Intelijen sebagai pengetahuan (*Intelligence as Knowledge)*: merupakan badan dari pengetahuan, Intelijen berhadapan dengan musuh, ataupun yang memiliki pontesi bermusuhan ataupun wilayah operasi memungkinkan untuk pengelola pengetahuan merencanakan dan memikul arahan organisasi.
- Intelijen sebagai proses (*Intelligence as Process)*: merupakan rangkaian

prosedur dan/atau langkah, kemudian membentuk siklus/lingkaran Intelijen (*Intelligence Cycle*), siklus tersebut berjalan awalnya dari munculnya permintaan jawaban atas sebuah pertanyaan dan/atau permintaan saran atas suatu permasalahan oleh pengambil keputusan.

Intelijen dalam istilah praktis dan akademis dibagi menjadi 3 (tiga) pengertian, yaitu:

1. Pengetahuan (*Knowledge*)
2. Aktifitas (*Activity*)
3. Organisasi (*Organization*)

Ketiga hal tersebut diatas merupakan masukan (input) bagi kebijakan dan strategi sehingga pengambil keputusan dapat menentukan sikap baik berupa pencegahan, penangkalan, dan penanggulangan terhadap semua ancaman yang ada, atas dasar produk Intelijen berupa deteksi dan peringatan dini (output) yang dihasilkan. Sehingga yang disebut dengan Pengetahuan (*Knowledge*) merupakan produk akhir dari Intelijen berupa deteksi dan peringatan dini, dan selanjutnya yang disebut dengan Aktifitas (*Activity*) merupakan kegiatan yang dilakukan oleh Intelijen dengan acuan proses siklus (*Intelligence Cycle*) baik secara terbuka maupun tertutup dan dilaksanakan oleh sebuah Organisasi (*Organization*) Intelijen.

Ancaman Siber

Ancaman dapat dikonsepsikan sebagai setiap usaha dan kegiatan, baik dari dalam negeri maupun luar negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa. Konsep ancaman mencakup hal yang sangat luas yaitu berupa tantangan, gangguan, dan hambatan serta spektrum yang senantiasa berkembang berubah dari waktu ke waktu. Ancaman terhadap kedaulatan negara yang semula bersifat konvensional (fisik) berkembang menjadi multidimensional (fisik dan nonfisik), baik yang berasal dari luar negeri maupun dari dalam negeri. Ancaman yang bersifat multidimensional tersebut dapat bersumber baik dari permasalahan ideologi, politik, ekonomi, sosial, budaya maupun permasalahan keamanan yang terkait dengan kejahatan internasional, antara lain terorisme, imigran gelap, bahaya narkotika, pencurian kekayaan alam, bajak laut dan perusakan lingkungan. Ancaman dibedakan menjadi dua yaitu ancaman militer dan ancaman nonmiliter. Ancaman terdiri atas dua komponen utama yaitu kemampuan dan niat. Kemampuan terdiri dari dua komponen turunan yaitu pengetahuan dan sumber daya, sedangkan niat dapat diukur dari dua hal yaitu keinginan dan harapan.

Siber adalah tempat yang sangat dinamis dan kompleks dimana kepentingan dan tindakan pribadi serta ketidaksengajaan secara luas mempengaruhi suatu hubungan dijalin. Siber sebagai suatu kondisi yang keberadaan utamanya dalam dunia virtual diciptakan oleh interaksi mesin-mesin komunikasi, atau yang terkenal dengan nama world wide web (www). Siber yaitu sekumpulan infrastruktur teknologi informasi dan komunikasi, aplikasi, dan peralatan dimana sebuah organisasi, perusahaan, atau misi bergantung, biasanya ditambah penunjang berupa internet, jaringan telekomunikasi, sistem komputer, peralatan pribadi, dan ketika terhubung dengan teknologi informasi, sensor, prosesor, dan mikrokontroler yang tertanam.

Ancaman adalah setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan, sehingga mengancam kerahasiaan, integritas dan ketersedian sistem dan informasi. Ancaman tersebut bisa berupa ancaman yang disengaja karena direncanakan dan/atau tidak disengaja seperti bencana serta ancaman yang muncul dari dunia siber. Ancaman yang muncul dari dunia siber ini dikenal sebagai ancaman siber. Ancaman siber adalah potensial peristiwa siber yang dapat menyebabkan hasil yang tidak diinginkan, yang mengakibatkan kerusakan pada sistem atau organisasi. Ancaman mungkin berasal dari luar atau internal dan mungkin berasal dari individu atau organisasi. Pada dasarnya ancaman siber dapat datang dari mana saja, dalam bentuk apa saja, dapat mengakibatkan gangguan yang berbeda-beda pada objek yang berbeda-beda pula. Ancaman siber pada dasarnya adalah suatu kondisi dalam dunia siber baik disengaja ataupun tidak yang dapat menimbulkan kerusakan, gangguan, kerugian, dan instabilitas pada infrastruktur teknologi informasi dan komunikasi.

Ancaman siber pada dasarnya dapat dibagi menjadi dua golongan yaitu ancaman siber yang tidak disengaja dan yang disengaja. Salah satu contoh ancaman siber yang tidak disengaja yaitu ketika memperbarui perangkat lunak atau pengelolaan prosedur yang tidak sengaja merusak sistem, sedangkan ancaman siber yang disengaja terdiri atas dua jenis yaitu serangan tertuju (serangan yang terjadi ketika suatu kelompok atau individu secara spesifik menyerang suatu aset siber) dan serangan tidak

tertuju (objek serangan tidak ditetapkan atau acak).

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif analisis. Penelitian kualitatif adalah penelitian yang datanya dinyatakan dalam bentuk verbal dan dianalisis tanpa menggunakan teknik statistik. Fokus penelitian dalam metode kualitatif dan yang diteliti untuk melihat sejauh mana sikap dan kebijakan yang direncanakan mampu menjejaskan keamanan nasional. Penelitian difokuskan pada faktor-faktor kerawanan keamanan, sikap dan kebijakan.

Proses yang dilakukan dalam penelitian ini memerlukan waktu dan kondisi yang berubah-ubah maka definisi penelitian ini akan berdampak pada desain penelitian dan cara-cara dalam melaksanakannnya yang juga berubah-ubah atau bersifat fleksibel. Jadi, penelitian yang dilakukan adalah penelitian kualitatif dengan tujuan penelitian deskriptif. Pendekatan kualitatif dipilih oleh peneliti data yang diperoleh berasal dari kajian literature (*library research*) atau studi kepustakaan dan wawancara terhadap informan. Penelitian ini bersifat deskriptif analitis melalui pengumpulan data secara terperinci dari berbagai sumber informasi, khususnya dari berbagai sumber yang berhubungan dengan objek kajian dalam penelitian ini.

Teknik Pengumpulan Data

Sebagaimana prosedur perolehan data penelitian kualitatif, maka data penelitian objek penelitian ini diperoleh dari studi kepustakaan dan wawancara. Studi kepustakaan dimaksudkan untuk memperoleh data dari berbagai referensi yang berhubungan dengan objek kajian peneliti. Sementara wawancara bertujuan untuk mendapatkan masukan data dari berbagai informan sebagai sumber yang berasal dari akademi (termasuk pengamat intelijen) dan praktisi (yang bekerja dan pernah bekerja dalam dinas intelijen) yang berhubungan dengan objek penelitian.

PEMBAHASAN

Kedudukan *Cyber Intelligence* dalam Bidang Intelijen

Dalam dunia intelijen, perhatian terhadap *cyber security* dan ancaman yang ditimbulkan dari dunia maya juga perlu semakin diprioritaskan. Terdapat beberapa kondisi penting yang perlu dipertimbangkan dalam menyikapi isu *cyber security* ini dalam dunia intelijen, yaitu:

1. Adanya kebutuhan dalam penggunaan jaringan internet dalam memperoleh, mengolah, dan menyimpan informasi dan data intelijen sehingga memerlukan pengamanan yang tinggi.
2. Perlunya kemampuan khusus dalam mengantisipasi dan mendeteksi serangan dunia maya (*cyber attack*) untuk kepentingan keamanan nasional.
3. Perlunya mengantisipasi jenis-jenis ancaman baru terhadap keamanan negara/nasional yang timbul dari kemajuan teknologi *cyber* seperti *cyber terrorism.*

Dalam bidang intelijen, isu *cyber security* juga menyangkut keberadaan *cyber espionage*. Keberadaan *cyber espionage* ini seringkali sulit untuk dideteksi karena meliputi penyisipan virus, *malware*, dan Trojan horses yang tidak dapat dikenali secara langsung (Zheng, 2015). Namun hal ini dapat diantisipasi melalui penguatan *cyber intelligence* khususnya bagi agen/badan intelijensi yang berwenang. Walaupun ilustrasi tentang *cyber security* menunjukkan kerentanan negara dan masyarakat terhadap ancaman dari dunia maya, intelijen dapat menjadi media yang bersifat tidak hanya defensif namun juga ofensif (Brantly, 2013). Dalam hal ini, penggunaan *cyber intelligence* harus mengambil peran utama dalam mengendalikan informasi *cyber* yang dapat dimanfaatkan untuk strategi keamanan. Dengan demikian, *cyber intelligence* memiliki kemampuan dalam memberikan masukan bagi pengambilan keputusan yang futuristik dan tidak selalu bersifat pasif untuk kepentingan protektif.

Cyber intelligence merupakan bentuk aktivitas intelijen yang dilakukan melalui jaringan komputer di dunia maya (Andress dan Winterfeld, 2014). Dengan semakin tingginya penggunaan media informasi melalui dunia maya ini maka Uthoff (2015) menyatakan bahwa *cyber intelligence* saat ini haruslah menjadi bagian yang integral dalam bidang intelijen. Oleh karena itu, *cyber intelligence* sewajarnya menempati posisi yang strategis karena kemampuannya mengumpulkan informasi dan data secara komprehensif dari sumber-sumber publik (*open source intelligence*/OSINT), media sosial (*social media intelligence*/SOCMINT), geospasial (*geospatial intelligence*/GEOINT), sinyal (*signal*

intelligence/SIGMINT), dan manusia (*human intelligence*/HUMINT).

Dalam kaitannya dengan intelijen nasional, secara eksplisit dalam UU NO. 17 tahun 2011 tentang Intelijen Negara, telah disebutkan bahwa intelijen negara merupakan lini pertama dalam sistem keamanan nasional yang mengemban peran dan fungsi pencegahan, penangkalan, dan penanggulangan setiap ancaman terhadap kepentingan dan keamanaan nasional. Peran dan fungsi yang besar ini memerlukan aktivitas intelijen yang ekstensif dan komprehensif termasuk dalam hal penggunaan kapasitas *cyber intelligence*. Di sisi lain, keberadaan ancaman terhadap keamanan nasional dari aktivitas dunia maya juga memerlukan kemampuan *cyber intelligence* yang tinggi dalam menangkal serangan melalui jaring informasi di dunia maya.

Namun hingga saat ini, pengaturan tentang pengelolaan keamanan dan ketahanan terhadap potensi bahaya dari dunia maya belum menjadi prioritas ancaman yang utama. Padahal tingkat serangan dunia maya di Indonesia meningkat 40% pada tahun 2017 dan menempatkan Indonesia sebagai salah satu negara dengan tingkat ancaman serangan dunia maya yang tinggi setelah Cina (Antaranews, 2018). Dalam mencermati kerentanan Indonesia terhadap *cyber attack* yang dapat mengancam keamanan nasional tersebut maka diperlukan pengaturan dan pengelolaan *cyber intelligence* yang memiliki payung hukum yang memadai.

Cyber Intelligence dalam Tata Kelola Intelijen Negara

Tata kelola keamanan siber di Indonesia masih bersifat parsial dan sektoral sehingga menyebabkan penanganan permasalahan keamanan siber belum terintegrasi dan belum terpadu. Hal tersebut menjadikan ancaman siber semakin nyata, terutama bila dikaitkan dengan ancaman ketahanan dan keamanan siber bagi pemerintah sebagai penyelenggara layanan publik sektor IIKN, pelaku ekonomi digital. Oleh karena itu, pengelolaan keamanan siber mutlak dilakukan secara terpadu untuk mencegah ancaman siber pada segala aspek kehidupan berbangsa dan bernegara. Terdapat beberapa organisasi pemerintah yang berurusan dengan komponen keamanan siber, seperti Kementerian Koordinator Bidang Politik, Hukum dan Keamanan (Kemenko Polhukam), Kementerian Komunikasi dan Informatika (Kominfo), Kementerian Pertahanan (Kemhan), Badan Intelijen Negara (BIN), Tentara Nasional Indonesia (TNI), dan Kepolisian Republik Indonesia (POLRI), serta Lembaga Sandi Negara (Lemsaneg) yang bertransformasi menjadi BSSN. Namun, berbagai program terkait keamanan siber yang disusun dan dilaksanakan masih pada level masing-masing instansi pemerintah dan belum ada titik fokus (focal point) formal sebagai pemegang komando koordinasi dan pengembangan keamanan siber di Indonesia. Saat ini telah terdapat inisiatif dari pemerintah untuk merencanakan pembentukan lembaga *cyber* nasional yang mengakomodasi kebutuhan akan *cyber intelligence* secara formal. Namun, hal penting yang juga perlu diwacanakan adalah menempatkan konteks *cyber intelligence* dalam tata kelola intelijen nasional. Hal ini menjadi penting karena terkait dengan sejumlah isu.

Pertama, penggunaan *cyber intelligence* haruslah menghasilkan informasi intelijen yang akurat dan berkualitas. Untuk kepentingan ini maka diperlukan sumber daya manusia dan teknologi yang memadai dalam melakukan pengumpulan dan pengolahan data intelijen dari sumber-sumber *cyber* media. Keakuratan menjadi penting karena, dengan *traffic* informasi yang cepat dan padat di dunia maya maka diperlukan kecermatan dalam menganalisis informasi yang ada. Sementara itu, secara defensif, kemampuan ini menjadi semakin penting sejalan dengan semakin meningkatnya kapasitas dan perkembangan teknologi yang digunakan dalam *cyber attack*.

Kedua, pengelolaan *cyber intelligence* pada lembaga-lembaga intelijen negara yang berwenang harus memiliki koneksi dan koordinasi yang jelas agar dapat dimanfaatkan dengan efektif. Permasalahan tumpang-tindihnya informasi intelijen yang diperoleh melalui dunia maya dari berbagai lembaga harus diperlakukan sebagai media triangulasi untuk menilai akurasi data intelijen yang diperoleh. Selain itu, kerja sama lintas negara dalam pertukaran dan pembagian *cyber intelligence* perlu pula diperkuat dengan tetap memperhatikan efektivitas serta menghormati prinsip-prinsip ataupun batasan yang telah disepakati tanpa terjebak dalam pertukaran aset intelijen yang dapat merugikan keamanan negara.

Ketiga, penggunaan *cyber intelligence* perlu menghindari terjadinya konflik dan ancaman terhadap *cyber freedom* bagi individu maupun kelompok yang justru dapat menciptakan suasana keamanan yang tidak kondusif. Dalih keamanan negara tidaklah menjadi dasar untuk membatasi kebebasan dalam dunia maya selama adanya bentuk aturan yang jelas, demokratis, dan sesuai dengan prinsip hak menyampaikan dan menyimpan informasi.

Keempat, aktvitas *cyber intelligence* perlu pula melibatkan komunitas *cyber intelligence*

yang digerakkan oleh aktor-aktor non-pemerintah karena kemampuan pemerintah merangkul komunitas ini dapat menjadi sumber daya yang besar dalam memberikan informasi intelijen. Komunitas ini memiliki jaringan non-formal yang luas dan global serta dapat dimanfaatkan untuk kepentingan keamanan nasional. Sebaliknya, mengambil posisi kontra terhadap komunitas tersebut dapat menjadi suatu potensi ancaman bagi pemerintah.

Kelima, penggunaan dan pengelolaan *cyber intelligence* yang memadai membutuhkan sumber dana yang tidak sedikit. Riset yang dilansir oleh Subrahmanian dkk (2015) menunjukkan bahwa negara-negara dengan tingkat *gross domestic product* (GDP) per kapita dan *human development index* (HDI) yang rendah memiliki kerentanan yang lebih tinggi terhadap serangan *cyber*. Dengan demikian, alokasi dana bagi kepentingan *cyber intelligence* harus mendapat perhatian yang penting pula. Tentunya hal ini menjadi suatu tantangan tersendiri bagi pemerintah mengingat masih minimnya anggaran bagi kebutuhan keamanan nasional khususnya dalam bidang intelijen. Untuk mengatasi hal ini maka perlu dikaji tingkat dan prioritas ancaman *cyber* yang utama maupun kebutuhan aktivitas *cyber intelligence* ofensif yang diperlukan sehingga dapat dialokasikan sumber dana pada aspek-aspek prioritas tersebut. Pada masa mendatang kebutuhan ini tentunya akan perlu dievaluasi mengingat dunia maya menjadi *battleground* yang semakin efektif dan produktif dengan perkembangan teknologi yang ada.

KESIMPULAN

Berdasarkan tulisan diatas dapat disimpulkan bahwa media siber mempunyai kerawanan yang bisa dimanipulasi bagi mengancam keamanan negara. Maka pihak pemerintah perlu mengambil langkah-langkah yang sewajarnya untuk mengelakkan siber menjadi medan mengancam keamanan nasional. Dengan memperhatikan sejumlah isu tersebut, maka peran *cyber intelligence* sebagai bentuk "baru" dalam tata kelola intelijen negara dapat menjadi lebih jelas dan menghindari permasalahan yang mungkin dapat timbul. Dalam hal ini, perhatian terhadap isu-isu ini harus dibarengi dengan adanya solusi dalam menyiapkan sumber daya manusia, infrastruktur, dana, dan teknologi yang mumpuni untuk dapat menjadikan *cyber intelligence* sebagai aset bagi kepentingan keamanan nasional dan negara.

DAFTAR PUSTAKA

Andress, J. dan Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practicioners*. Waltham: Esevier.

Bisson, D. (2015). A "Cyber" Study of the U.S. national Security Strategy Reports. Diakses Dari https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-us-national-security-strategy-reports/

Brahmanian, V.S., Ovelgonne, M., Dumitras, T., dan Prakash. A. (2015). The Global Cyber-Vulnerability Report. Switzerland: Springer International Publishing

Brantly, A. (2013). Defining the role of intelligence in cyber: A hybrid push and pull. Dalam Mark Phytian (Ed.). Understanding the Intelligence Cycle, pp. 76 - 98. Oxon: Routledge

Caplan, N. (2013). Cyber War: the Challenge to National Security. Global Security Studies, 4 (1), 93 -115

Graham, S. (2010). When Infrastructures Fail. Dalam Stephen Graham (Ed). Disrupted Cities: When Infrastructure Fails, pp. 1- 26. New York: Routledge

Irawan Sukarno, 2011, Aku Tiada Aku Niscaya, Menyingkap Lapis Kabut Intelijen, Buku Obor, Jakarta

Lindsay, J.R. (2015). China and cybersecurity: Contoversy and context. Dalam Jon. R. Lindsay, Tai Ming Cheung, dan Derek S. Reveron (Eds). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, pp. 1 - 28. New York : Oxford University Press

Supono Soegirman, April 2013, Etika Praktis Intelijen, Dari Sungai Tambak Beras Hingga Perang Cyber, Media Bangsa, Jakarta

Undang-Undang No.17 tahun 2011 tentang Intelijen Negara

Uthoff, C. (2015). Strategic Cyber Intelligence: An examination of Practices across Industry, Government, and Military. Dalam Frederic Lemieux (Ed.). Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice. Hampshire: Palgrave Macmillan

Zheng, Y. (2015). From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. Dalam Jon. R. Lindsay, Tai Ming Cheung, dan Derek S. Reveron (Eds). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, pp. 123 - 128. New York : Oxford University Press