Digitimes #21
APRIL 2019

STRATEGI KEAMANAN SIBER INDONESIA

REKOMENDASI RENCANA AKSI DAN IMPLEMENTASI

WSIS PRIZES 2018 CHAMPION www.wsis.org

CfDS
CENTER FOR DIGITAL SOCIETY

Room BC 201- 202
Faculty of Social and Political Sciences
Universitas Gadjah Mada
Jalan Sosio Yustisia 1, Bulaksumur, Yogyakarta
(0274) 563362, Ext. 116 | cfds.fisipol@ugm.ac.id

PENELITI DAN KONTRIBUTOR

Tim Penulis

Anggika Rahmadiani
Anisa Pratita Kirana Mantovani
Syauqy Uzhma Hariz
Janitra Haryanto
Faadilah Fayyadh Aidad

Editor

Treviliana Eka Putri

Desain dan Tata Letak

Naufal Alatas Radityasakti

April 2019

DAFTAR ISI

Photo by Jenna Jacobs on Unsplash

PENDAHULUAN

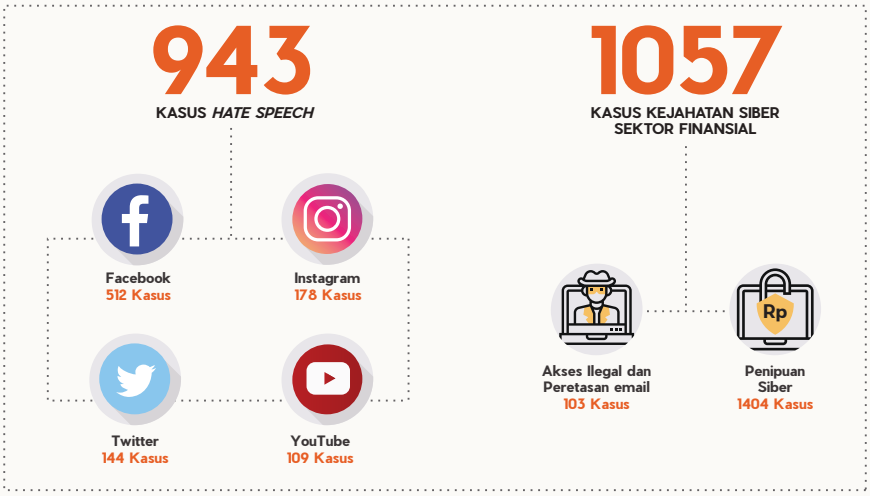
Menurut *International Telecommunication Union* (ITU) dalam publikasinya, "*Understanding Cybercrime: A guide for Developing Countries*", kejahatan siber didefinisikan sebagai sebuah bentuk kejahatan dimana komputer dan jaringan digunakan sebagai tempat terjadinya tindak kriminal, target, maupun alat untuk melakukan tindak kriminal.[1] Berdasarkan pelanggaran yang dilakukan, kejahatan siber diklasifikasikan ke dalam lima tipologi: (1) serangan terhadap kerahasiaan, integritas dan ketersediaan data dan sistem komputer, (2) serangan yang berkaitan dengan komputer, (3) serangan yang berkaitan dengan konten, (4) serangan yang berkaitan dengan pelanggaran hak cipta dan sejenisnya.[2] Tipologi ke (1), (3) dan (4) berfokus pada peraturan hukum yang dilanggar sedangkan tipologi ke (2) berfokus pada metode serangan yang dilakukan.[3] Oleh sebab itu, sebuah kejahatan siber tidak selalu dapat dikategorikan dalam satu kategori saja, melainkan dapat dikategorikan dalam berbagai kategori tipologi yang tersedia.

Saat ini, kejahatan siber masih menjadi ancaman bagi pemerintah negara-negara di seluruh dunia, khususnya pemerintah Republik Indonesia (RI). Pasalnya, selain karena pola dan bentuk kejahatan siber masih terus berkembang setiap waktunya, kejahatan siber dapat menyebabkan dampak yang sangat luas, mulai dari dirugikannya individu hingga sebuah negara. Menurut pemaparan Komisaris Besar (Kombes) Bareskrim Polri Ricky pada Convention on Cybersecurity 2018

yang diadakan oleh CfDS UGM, terdapat tiga bentuk kejahatan siber yang paling marak dilakukan di Indonesia: *hate speech*; kejahatan siber yang berhubungan dengan finansial, seperti akses ilegal, penipuan dan peretasan email perusahaan; dan kejahatan yang berhubungan dengan *financial technology* (fintech).[4]

Kasus *hate speech* dilakukan oleh pengguna media sosial pada *platform* media sosial, dengan jumlah 512 kasus terjadi di Facebook, 178 kasus terjadi di Instagram, 144 kasus terjadi di Twitter dan 109 kasus terjadi di YouTube.[5] *Hate speech* dikategorikan sebagai kegiatan-kegiatan yang berbentuk *hoax*, makar, narkoba, penghinaan, penipuan, pidana umum, pornografi, provokasi, radikalisme dan SARA. Tindakan *hate speech* seringkali dilakukan dengan berbagai motif, baik untuk menyerang individu lainnya maupun untuk mencapai tujuan politiknya.

Mengenai kejahatan siber yang berhubungan dengan sektor finansial, Bareskrim Polri mencatat 1507 kasus yang terkait dengan akses ilegal, penipuan dan peretasan email perusahaan. Dari 1507 kasus tersebut, 1404 kasus merupakan penipuan siber dan sisanya merupakan kasus akses ilegal dan peretasan email perusahaan. Dalam menjalankan aksinya, para pelaku penipuan siber biasanya menggunakan teknik-teknik penyalahgunaan komputer, seperti menjebol (*cracking*), mengacak data (*diddling*), membocorkan data (*leaking*), menolak memberikan pelayanan serangan (*denial of service attack*), menyamar atau meniru, memalsukan dan mengancam e-mail (*email forgery and threat*) dan menyusup (*piggybacking*).[6]



Dalam beberapa kasus kejahatan siber yang berhubungan dengan sektor finansial dan terkait dengan jasa perbankan, kelemahan sistem jaringan perbankan juga dapat memberikan celah para pelaku kejahatan siber untuk melakukan pembelian barang di *platform* e-dagang tanpa mengurangi jumlah saldo yang berada dalam rekeningnya. Metode manipulasi transaksi yang terungkap oleh Bareskrim polri menunjukkan bahwa ketika alamat situs *internet banking* tidak mengantisipasi penghapusan *script* pilihan transaksi, pelaku dapat meretas alamat situs tersebut untuk menghapus *script* pilihan transaksi sehingga dianggap transaksi masih dianggap wajar dan diverifikasi oleh pihak toko online.[7]

Kejahatan siber yang dijelaskan di atas adalah bentuk kejahatan siber yang hanya merugikan individu atau kelompok-kelompok tertentu. Ancaman siber yang muncul selain ancaman internal yang menyasar warga negara pada level individu adalah ancaman eksternal. Ancaman eksternal adalah ancaman yang dihadap oleh sebuah negara terhadap serangan dari luar negara tersebut. Ancaman eksternal dapat berbentuk perang siber, serangan siber dan spionase siber. Perang dan spionase siber memiliki dampak yang lebih luas, yakni pada tingkat negara.

Sebagai contoh, serangan virus Stuxnet yang dilakukan oleh pemerintah Israel dengan dukungan Amerika Serikat (AS) terhadap pemerintah Iran di fasilitas nuklir Iran di Natanz. Serangan siber tersebut digunakan oleh badan intelijen Israel Mossad sebagai opsi yang lebih aman untuk dilakukan dibandingkan dengan mengebom fasilitas nuklir Iran yang ditakutkan akan meningkatkan kekerasan atau serangan balik yang dapat dilakukan Hezbollah, Hamas maupun Suriah.[8] Serangan Stuxnet berhasil menghambat perkembangan nuklir Iran dan menaikkan posisi tawar Israel di mata Iran. Contoh

lainnya adalah serangan virus WannaCry di Inggris pada tahun 2017 yang mengakibatkan kelumpuhan fasilitas medis karena terblokirnya data-data medis masyarakat Inggris.[9] Serangan siber yang terjadi di Inggris dan Iran membuktikan bahwa kejahatan siber dapat mengubah posisi tawar sebuah negara di mata internasional dan mengancam keberlangsungan hidup masyarakat sebuah negara.

Kedua ancaman siber diatas, baik internal dan eksternal telah disadari oleh pemerintah RI. Sebagai respon atas berkembangnya ancaman siber di Indonesia, di awal tahun 2018, pemerintah RI membentuk Badan Siber dan Sandi Negara (BSSN), institusi yang bertanggungjawab kepada presiden untuk meningkatkan keamanan siber di Indonesia dan menanggulangi berbagai ancaman siber di Indonesia. Pembentukan BSSN merupakan langkah awal yang baik bagi pemerintah RI untuk menjaga kedaulatan RI di ranah dunia maya. Namun, langkah tersebut perlu ditindaklanjuti dengan pembuatan kerangka koordinasi yang komprehensif dan melibatkan berbagai pemangku kebijakan di Indonesia untuk melawan ancaman siber nasional.

Saat ini, menurut pemaparan Direktur Proteksi IIKN BSSN Agung Nugraha, BSSN telah menyusun strategi keamanan siber nasional dan sedang dikumpulkan ke ITU. Selain itu, menurut publikasi BSSN, beberapa *Memorandum of Understanding* (MoU) telah diresmikan BSSN dengan berbagai lembaga pemerintah. Sebagai contoh, BSSN dengan Kementerian Kesehatan (Kemenkes) RI melalui MoU menyepakati adanya pemanfaatan sertifikat elektronik untuk meningkatkan keamanan transaksi elektronik, pengamanan teknologi informasi dan komunikasi, peningkatan dan pengembangan sumber daya manusia, pertukaran informasi dan pemanfaatan lain yang disepakati oleh BSSN dan Kemenkes RI.[10] Namun begitu, Indonesia belum memiliki kerangka koordinasi antarinstitusi yang komprehensif dan integratif, serta belum memiliki standar untuk menetapkan kebijakan keamanan siber.

Oleh sebab itu, kami mengajukan rekomendasi kerangka kerjasama yang komprehensif dan berbasis *multi-stakeholder* untuk memastikan tingkat keamanan siber yang kuat. Kerangka koordinasi yang komprehensif dan berbasis *multi-stakeholder* menjadi penting mengingat saat ini kebijakan keamanan siber di Indonesia masih bersifat sektoral dan belum memiliki standar nasional. Ketiadaan standar nasional ini juga menyebabkan absennya institusi yang dapat mengawasi tingkat keamanan siber di Indonesia.

Dalam rekomendasi yang kami ajukan, kami mengikutsertakan empat unsur negara yang terdiri dari: sektor pemerintahan, sektor industri, sektor masyarakat dan sektor akademisi. Dalam konsep kerangka koordinasi yang kami rancang, kami menempatkan BSSN sebagai institusi coordinator yang menetapkan standar nasional bagi kebijakan keamanan siber institusi-institusi pemerintahan lainnya seperti berbagai kementerian, Badan Usaha Milik Negara (BUMN), pemerintah daerah, serta industri-industri Indonesia, seperti penyedia jasa finansial dan *fintech*.

Dalam penyusunan rekomendasi strategi nasional ini, perusahaan konsultan keamanan siber dilihat sebagai pihak yang dapat memberi masukan dan me-review standar nasional yang ditetapkan oleh BSSN. Selain konsultan keamanan siber, kami juga menempatkan kelompok akademisi sebagai pihak yang menyediakan akreditasi dan sertifikasi bagi institusi-institusi yang nantinya akan berada di bawah pengawasan BSSN dalam hal keamanan siber. Unsur-unsur masyarakat seperti lembaga swadaya masyarakat yang memiliki kepedulian terhadap keamanan siber juga diikutsertakan sebagai pihak yang dapat memberikan masukan kepada pemerintah serta menjadi perpanjangan tangan pemeirntah untuk mensosialisasikan keamanan siber yang sesuai dengan standar nasional yang ditetapkan oleh BSSN. Nantinya, dalam menindaklanjuti ancaman-ancaman siber, BSSN juga akan berkoordinasi dengan POLRI dan TNI sebagai pihak yang memiliki wewenang lebih lanjut dalam menginvestigasi dan menangani kasus ancaman siber.

Riset yang kami lakukan untuk menyusun kerangka koordinasi antar lembaga tersebut menggunakan metode penelitian *desk research* – dengan menggunakan data sekunder yang telah dirilis seara publik. Kami mengumpulkan data-data melalui review literatur-literatur yang membahas mengenai keamanan siber seperti buku, jurnal ilmiah, berita, artikel daring dan publikasi-publikasi pemerintah. Selain itu, kami juga menggunakan data-data yang didapatkan dari pemaparan para pemangku kebijakan, perwakilan korporasi, serta akademisi yang memberikan materi dalam sesi-sesi Convention on Cybersecurity 2018 di Universitas Gadjah Mada, Yogyakarta.

KAPASITAS KEAMANAN SIBER INDONESIA

Urgensi regulasi keamanan siber di Indonesia hadir salah satunya disebabkan oleh tingginya pengguna internet. Data menyebutkan bahwa pengguna internet di Indonesia saat ini sejumlah 143,26 juta jiwa, dimana angka tersebut sebanding dengan 54,68 persen jumlah penduduk keseluruhan.[11] Tingginya pengguna internet tersebut ditambah lagi dengan adanya prediksi jumlah pertumbuhan pengguna internet yang tinggi, yakni lebih dari 8 persen pertahun. Hingga tahun-tahun mendatang, diperkirakan terdapat tren positif terhadap pengembangan jumlah pengguna internet di seluruh Indonesia. Dengan demikian, dampak dan manfaat yang diterima masyarakat atas penggunaan internet pun kian luas. Di sisi lain, dengan tingginya penetrasi pengguna internet di Indonesia, turut berkorelasi dengan tingginya tingkat risiko kejahatan berbasis internet.

Kekhawatiran akan hadirnya berbagai ancaman baru yang muncul dari persebaran pengunaan internet muncul seiring dengan meningkatnya intensitas penggunaan teknologi dan menimbulkan urgensi pembentukan institusi ataupun regulasi baru terkait keamanan siber. Hal tersebut tertuang pula dalam kesepakatan dalam forum PBB yang bernama United Nations Group of Governmental Experts (UN-GGEs). Beberapa kesepakatan di dalamnya menguraikan adanya dukungan untuk menciptakan norma siber baru.[12] Poin-poin detailnya menegaskan bahwa negara-negara harus memasukkan aspek ICT (*Information Communication Technology*) sebagai hal yang perlu diseriusi dalam beberapa kerangka kebijakan yang melindungi warga dunia dari ancaman.

Menurut laporan yang dirilis oleh Norton, hingga tahun 2017 saja terdapat sekitar 57.4 juta orang di Indonesia yang menjadi korban dari serangan siber.[13] Kerugian yang dialami entitas bisnis dan korporasi yang diakibatkan oleh serangan siber pun sangat besar. Berdasarkan laporan yang dirilis oleh Microsoft pada tahun 2017, kerugian yang harus ditanggung perusahaan-perusahaan di Indonesia akibat kejahatan siber mencapai lebih dari 33 Miliar Rupiah.[14] Sementara dalam kajian yang dilakukan oleh *Global Partners Digital*, disebutkan bahwa dalam kasus peradilan di Indonesia yang menggunakan UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dalam delik perkara meningkat hingga 60 kasus pertahun di tahun 2015.[15] Hal ini ikut mengindikasikan bahwa ancaman siber sudah kian merebak. Sulitnya menangkal ancaman ini disebabkan oleh latennya sistem dunia siber yang membutuhkan sistem penanganan khusus yang komprehensif dalam aplikasinya. Di sisi lain, tidak adanya regulasi hukum yang spesifik mengatur tentang keamanan siber menjadi pekerjaan rumah bagi pemerintah dalam menindak ancaman-ancaman siber yang laten.

57,4 Juta
orang Indonesia menjadi korban serangan siber

Rp.33 Miliar
Kerugian yang ditanggung perusahaan-perusahaan di Indonesia akibat kejahatan siber

Seiring dengan berkembangnya tren kepedulian dunia terhadap keamanan siber, beberapa kali organisasi dunia menyelenggarakan penilaian terhadap kapasitas penyelenggaraan keamanan siber di seluruh dunia. Pada tahun 2017 dan 2018 setidaknya terdapat dua lembaga yang melalukan *assesment* terhadap pelembagaan keamanan siber di Indonesia. Lembaga Uni Telekomunikasi Internasional (ITU) menyelenggarakan penilaian Global Cybersecurity Index (GCI) di tahun 2017. Dari penilaian tersebut, Indonesia berada di posisi ke 70 dari 162.[16] Dalam penilaian tersebut, terdapat lima indikator pelembagaan keamanan siber yang dinilai dari suatu negara di antaranya: *Legal, Technical, Organizational, Capacity Building, Cooperation.* Sedangkan yang terbaru di tahun 2018, E-Governance Academy (EGA) melakukan hal serupa dengan istilah *National Cyber Security Index* (NCSI). Dari penilaian tersebut, Indonesia berada di posisi 83 dari 100 negara.[17] Dalam data yang disajikan tersebut, empat hal yang didalami adalah *Legislation in force, Established units, Cooperation formats,* dan *Outcomes/ Product.*

Bagaimanakah sebenarnya kapasitas pemerintah Indonesia dalam menghadapi ancaman-ancaman baru dalam keamanan siber?

Kapasitas Organisasional: Pembentukan Badan Siber dan Sandi Negara (BSSN)

Pada awal tahun 2017 pemerintah Republik Indonesia menerbitkan Peraturan Presiden (Perpres) nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara. Terbitnya Perpres tersebut merupakan sebuah langkah besar di tengah semakin meningkatnya urgensi terhadap peraturan terkait keamanan siber yang komprehensif. Badan Siber dan Sandi Negara (BSSN) ini dibentuk untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.[18] Badan tersebut dibentuk langsung oleh pemerintah, bertanggung jawab kepada presiden, dan difungsikan untuk menyelenggarakan penciptaan iklim siber yang aman.

Kapasitas Legal: Undang-Undang dan Peraturan terkait Keamanan Siber

Selain peraturan yang berkaitan dengan aktivitas kejahatan/ kriminal, hal-hal yang terkait dengan keamanan siber di Indonesia hanya bertumpu pada 3 regulasi. Pertama adalah Undang-undang (UU) nomor 36 tahun 1999 tentang Telekomunikasi.[19] Peraturan ini mengatur tentang bagaimana Telekomunikasi dilaksanakan dengan andal. Melengkapi regulasi tersebut, ada pula UU nomor 11 tahun 2008[20] tentang Informasi dan Transaksi Elektronik yang pula dilengkapi oleh UU nomor 19 tahun 2016[21] tentang perubahan atas UU nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Ditambah pula oleh Peraturan Pemerintah (PP) no 82 tahun 2012[22] tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Ketiga aturan tersebut secara simultan melengkapi penyelenggaraan kegiatan siber di Indonesia. Poin tentang bagaimana keamanan siber dilembagakan secara umum, belum tertuang dalam aturan khusus yang baku.

Di sisi legal ataupun regulasi yang diterapkan pemerintah, UU Keamanan dan Pertahanan Siber juga sudah menjadi 1 dari 55 proglam legislasi nasional (prolegnas) yang berarti akan menjadi prioritas untuk dibentuk menjadi undang-undang.[23] Dalam regulasi lain, terdapat revisi di UU ITE di tahun 2016 serta adanya wacana revisi dalam Peraturan Pemerintah nomor 82 tahun 2012 sedang berjalan. Kedua aspek regulasi maupun kelembagaan secara organisasi menimbulkan titik terang bagi kemajuan keamanan siber Indonesia di masa depan.

Terkait dengan standar dan regulasi tentunya tidak dapat dipisahkan dari perkembangan sektor bisnis dan swasta. Regulasi dan standar dipandang sebagai unsur penting yang dapat membangun kejelasan mekanisme bisnis yang dijalani. Selama ini, nyatanya sektor swasta adalah sektor yang paling membutuhkan sistem informasi dan jaringan erat terkait dengan penerapan teknologi. Azas efektif dan efisien yang selalu dibutuhkan oleh perusahaan, menuntut penggunaan ICT di perusahaan akan selalu terjadi. Standardisasi penyelenggaraan jaringan yang aman sudah lebih dahulu diterapkan di perusahaan. ISO 27001 tentang keamanan jaringan merupakan tren standarisasi mutu yang sudah berkembang di Indonesia. Audit dan penyeragaman mutu sudah dilakukan secara masif dan hampir di seluruh perusahaan yang menggunakan jaringan internet. Standarisasi mutu untuk keamanan siber secara khusus terus berkembang. Sebagai contoh, lahirnya ISO 27301 secara khusus menjelaskan standarisasi mutu terkait ICT *readiness for business continuity*[24]. Didalamnya memuat terkait aspek ICT apa saja dan resiko-resikonya terkait dampaknya terhadap keberlanjutan usaha. Termasuk didalamnya terkait aspek keamanan yang sudah diperbarui.

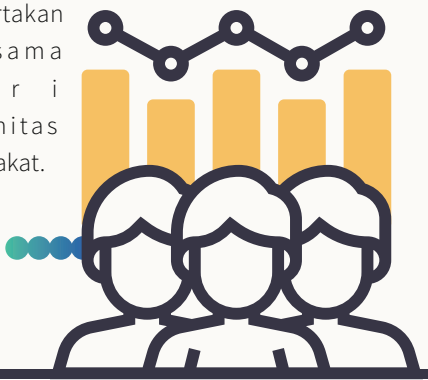
Kapasitas Kerjasama Antarlembaga

Kerjasama antarlembaga terkait dengan isu keamanan siber dilihat masih belum terjalin dengan baik. Belum adanya alur regulasi koordinasi yang jelas antarinstitusi dan antarsektor merupakan penyebab lemahnya kerjasama tersebut. Salah satu poin terberat dalam melembagakan keamanan siber menjadi hal yang berjalan secara sistemik dan menyeluruh di Indonesia terkait erat dengan aspek koordinasi. Logika pemerintahan Indonesia yang birokratik dan cenderung kaya akan struktur ketimbang fungsi, menjadi tantangan berat. Terdapat tantangan untuk berkoordinasi dan membuat alur kerja baik kelembagaan terkait dengan *stakeholder* lintas instansi baik pemerintah, swasta, maupun masyarakat. Hal ini juga terkait dengan bagaimana isu-isu sektoral yang berbeda kebutuhan satu sama lain bisa dikoordinasikan secara berimbang dan proporsional.

Kapasitas Sumber Daya Manusia/Masyarakat

Sumber daya manusia dilihat sebagai salah satu faktor penting yang dapat mendukung terciptanya ekosistem keamanan siber di Indonesia. Sumber daya manusia yang dimaksud mencakup komunitas masyarakat sebagai pengguna teknologi yang rentan terhadap ancaman siber dan juga sebagai tenaga ahli professional yang dibutuhkan dalam keamanan dan pertahanan siber. Minimnya tenaga ahli di bidang keamanan siber di Indonesia seringkali disebut sebagai sebuah tantangan yang paling besar terhadap penguatan ekosistem keamanan siber nasional.[25] Selain itu, minimnya budaya keamanan siber dalam masyarakat Indonesia juga dilihat sebagai sebuah ancaman yang cukup urgen. Natur ranah siber yang memungkinkan terjadinya serangan kritis yang berasal dari kelalaian individu menjadikan pembangunan budaya keamanan siber sebagai sebuah fondasi penting.

Perlu terdapat peningkatan pemahaman atas pentingnya peran dan partisipasi masyarakat dalam meningkatkan keamanan siber. Selain terkait pertahanan dan keamanan negara, di sisi lain, isu terkait dengan hak personal ataupun perlindungan data pribadi tidak pernah dipisahkan dari diskursus keamanan siber. Hal inilah yang menjadi tolak ukur betapa masyarakat pun memiliki andil yang besar. Regulasi dan pelembagaan perlu menyertakan kerjasama dari komunitas masyarakat.



Kapasitas Teknis/ Infrastruktur

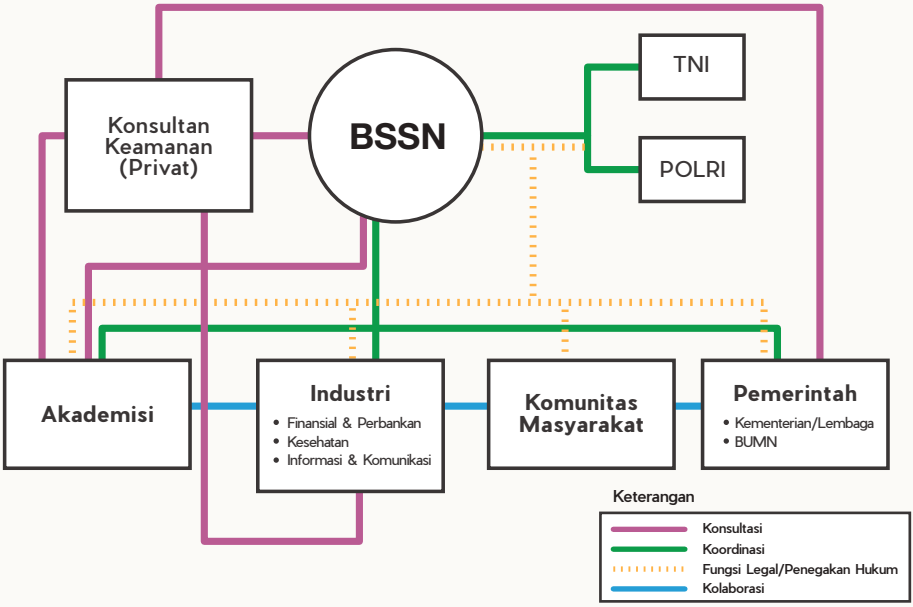
Aspek teknis masih merupakan kendala dan pekerjaan rumah yang besar bagi Indonesia. Keamanan siber mencakup dua aspek penting, yaitu infrastruktur lunak dan keras. Infrastruktur lunak mencakup Sumber Daya Manusia (SDM), kebijakan, proses, protokol, dan pedoman untuk melindungi sistem dan data. Sementara itu, yang dimaksud dengan perangkat keras adalah teknologi yang dibutuhkan untuk melindungi sistem dan data dari ancaman eksternal dan internal siber.[26] Menurut *Global Cybersecurity Index*, Indonesia masih tertinggal di sektor teknis dalam pembangunan CERT/CSIRT Sektoral.[27] Kelemahan kapasitas teknis tersebut perlu diatasi dengan komitmen yang lebih kuat dari pemerintah maupun sektor terkait terhadap pengadaan infrastruktur yang dibutuhkan untuk menjaga keamanan siber, baik dari segi *hardware* maupun peningkatan kapasitas sumber daya manusia yang dapat melindungi infrastruktur tersebut dari kelalaian dan kerentanan yang dapat dieksploitasi oleh peretas.

Dengan berdirinya BSSN, Indonesia telah memenuhi pilar organisasional yang dicetuskan oleh ITU. Namun berdirinya BSSN saja tidaklah cukup untuk memiliki sebuah *framework* keamanan siber yang efektif. Maka dari itu, bahkan dalam pelaksanaan BSSN sebagai sebuah organisasi, dibutuhkan kecakapan SDM, kerjasama dan koordinasi yang harmonis antarlembaga, regulasi hukum yang jelas, serta perangkat teknologi yang mumpuni.

REKOMENDASI KERANGKA KERJASAMA KEAMANAN SIBER INDONESIA

Berangkat dari penilaian atas kapasitas pemerintah terhadap lima indikator keamanan siber tersebut diatas, maka dibutuhkan sebuah *framework* kerjasama *multistakeholder* yang bersifat multidimensional. Empat sektor utama yang dilihat penting perannya dalam pelaksanaan kerangka keamanan siber di Indonesia dalam hal ini adalah sektor akademik, bisnis, pemerintah, dan juga komunitas masyarakat.[28] BSSN telah memiliki sebuah skema kerjasama yang melibatkan sektor- sektor tersebut, namun hingga saat ini masih sedikit dokumen pendukung yang dapat ditemukan yang menjelaskan koordinasi factual antarinstitusi tersebut. Maka dari itu, penulis berusaha untuk menjabarkan apa yang dimaksud dengan masing- masing sektor tersebut dan bagaimana peranannya dalam skema kerjasama keamanan siber. *Framework* kerjasama ini didasarkan oleh elaborasi data temuan yang ditemukan oleh Puslitbang Kominfo[29] dan juga *Global Cybersecurity Agenda* (GCA) yang dikeluarkan oleh ITU.

Rekomendasi
Skema Koordinasi Multisektoral



A. Badan Siber dan Sandi Negara (BSSN)

BSSN merupakan instansi badan nasional pengembangan dari Lembaga Sandi Negara. BSSN disahkan melalui Perpres Nomor 53 tahun 2017 yang selanjutnya disempurnakan melalui Perpres Nomor 133 tahun 2017. dalam kerangka Strategi Keamanan Siber Nasional-nya, BSSN juga telah mengidentifikasi enam sektor yang rawan terkena serangan siber, yaitu pemerintahan, pertahanan dan keamanan, perbankan, kesehatan, ESDM, transportasi, TIK, dan ketahanan pangan. Dalam *framework* kerja sama *multi-stakeholders* di atas, BSSN berperan sebagai koordinator. Sebagai koordinator, hal paling mendasar yang patut untuk dilakukan oleh BSSN adalah perumusan kebijakan strategis mengenai keamanan siber dan responnya dan juga standardisasi pengaturan keamanan siber.[30] Selain itu, tujuan utama dari pembuatan skema kerja sama diatas adalah penguatan BSSN sebagai instansi yang bertanggung jawab atas segala isu yang menyangkut dengan siber dan sandi. Arus kerja sama yang tergambar adalah kerja sama dua arah, di mana BSSN diharapkan dapat mensosialisasikan isu-isu siber dan sandi kepada lima *stakeholders* lainnya. Sebaliknya, terdapat arus koordinasi balik dari lima *stakeholders* tersebut kepada BSSN yang akan dijabarkan dalam kelima poin dibawah ini, sesuai dengan sektor masing- masing.

B. Instansi Pemerintah

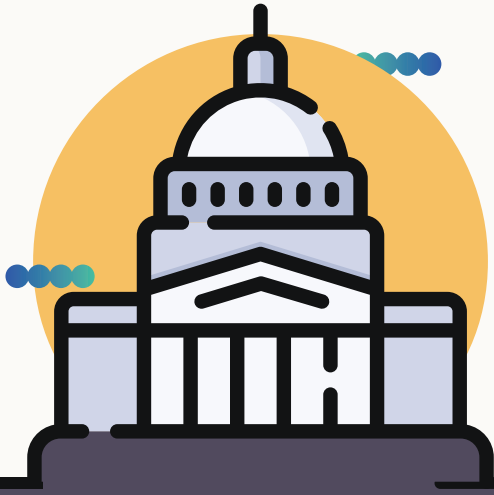
Di dalam sebuah skema kerja sana *multi-stakeholders*, salah satu kekhawatiran yang muncul adalah melemahnya peranan instansi pemerintah, dan menguatnya sektor swasta.[31] Namun sebetulnya, peran pemerintah di sini sangatlah krusial. Pemerintah sebagai wakil negara memiliki kewenangan untuk mengumpulkan data intelijen dari negara lain.[32] Pemerintah juga dapat merahasiakan informasi – dari entitas lain di luar pemerintahan – sebelum informasi tersebut tersedia untuk swasta maupun masyarakat luas. Selain itu, sangat penting bagi instansi pemerintah disini untuk memiliki kewaspadaan akan keamanan siber, mengingat sektor pemerintahan merupakan salah satu sektor yang teridentifikasi rawan mendapat serangan siber. Namun sayangnya, hingga saat ini hanya dua kementerian yang sudah memiliki CERT sendiri.

Pertama, Kementerian Informasi dan Komunikasi (Kemkominfo) yang sudah mendirikan ID-SIRTII, kepanjangan dari *Indonesia Security Incident Response Team on Internet Infrastructure*. Lembaga ini didirikan pada tahun 2007 berdasarkan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi berbasis Protokol Internet. ID SIRTII merupakan *response team* tingkat nasional yang memiliki empat level prioritas dalam penanganan insiden. Prioritas pertama diberikan kepada insiden yang dampaknya dapat berakibat pada terganggunya keamanan publik dan keamanan negara. Prioritas kedua adalah penanganan insiden yang berdampak pada perekonomian negara. Prioritas ketiga diberikan pada insiden yang dirasa dapat menimbulkan kerugian politis, dan prioritas terakhir adalah penanggulangan insiden yang merugikan aspek sosial-budaya.[33]

Selain Kemkominfo, Kementerian Pertahanan (Kemenhan) juga memiliki COC, *Cyber Operation Center*. COC merupakan embrio dari pertahanan siber Kemhan. Selain itu, COC juga bertanggungjawab untuk melakukan pembangunan, pengoperasionalan, pemeliharaan dan pengembagan sistem pertahanan siber Kemhan Saat ini, COC telah bergant nama dengan Pusat Operasi Pertahanan Siber. Sementara itu, untuk tigkat provinsi dan kabupaten, hanya Provinsi Jawa Barat dan Jawa Timur yang sudah memiliki CERT sendiri. Kerjasama yang terjalin oleh BSSN dan instansi pemerintah lainnya saat ini terbatas pada kerjasama penggunaan *e-certificate* sebagai upaya pengamanan data diri dan arsip. Sebagai contoh, kerjasama telah dijalin dengan Kementerian kesehatan, Kementerian Riset, Teknologi dan

Pendidikan Tinggi, Kementerian ATR/BPN,dan beberapa Pemerintah Daerah. Dengan demikian, dapat dikatakan bahwa sebenarnya sektor pemerintahan Indonesia masih sangat rentan terhadap serangan siber. Sikap antisipatif dan preventif dari instansi pemerintah masih jauh dari cukup. Maka dari itu, BSSN perlu untuk memperkuat sistem pertahanan siber negara baik melalui program sosialisasi maupun pelatihan.

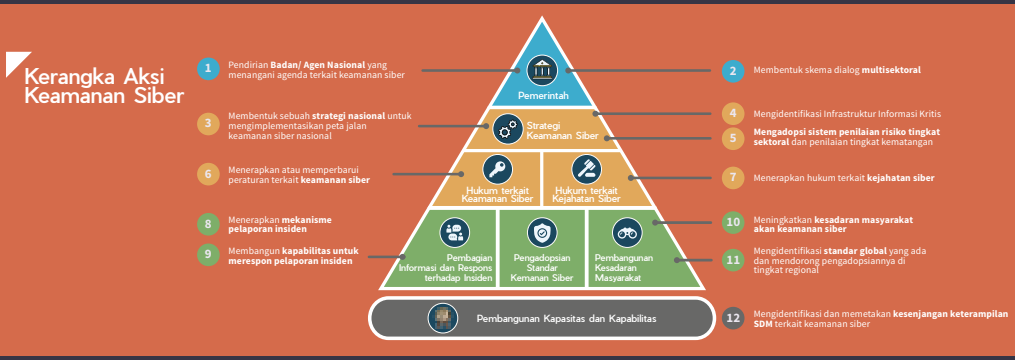
Permasalahan selanjutnya adalah kurangnya dokumen legal atau undang-undang yang mengatur tentang keamanan siber di Indonesia. Melihat dinamika ancaman siber yang semakin mengkhawatirkan, koordinasi yang dapat dilakukan oleh BSSN dengan pemerintah selanjutnya adalah penguatan undang-undang yang mengatur tentang keamanan siber dan juga mempercepat RUU terkait. Tata kelola perundang-undangan keamanan siber sangat diperlukan sebagai pedoman kerja BSSN dalam memperkuat sistem keamanan siber negara. Sampai saat ini, masih ada dua RUU yang masih dipersiapkan, yaitu RUU Perlindungan Data Pribadi dan RUU Keamanan Siber. Keduanya diharapkan dapat dimasukan dalam Program Legislasi Nasional 2019.



C. *Industri Penyedia Jasa Konsultasi Keamanan Siber*

Di dalam skema kerja sama *multi-stakeholders* yang dimiliki oleh BSSN, tidak terdapat sektor industri konsultan keamanan. Padahal, industri konsultan ini sangat penting perannya dengan adanya kemampuan teknologi dan sumber daya manusia yang sangat memadai. Di dalam skema kerjasama di atas, BSSN melaksanakan fungsi konsultatif dengan perusahaan konsultan untuk mengawasi ekosistem siber dengan harapan dapat tercipta keamanan, pertahanan siber, dan pemulihan sistem apabila sewaktu-waktu terjadi serangan siber. Perusahaan-perusahaan dengan kapasitas sumber daya manusia dan juga teknis yang baik diharapkan dapat merencanakan skema perlindungan dengan berpikir layaknya penyerang dan juga target korban untuk membangun solusi keamanan terbaik yang dibutuhkan.[35]

Saat ini, pemerintah Indonesia sedang meningkatkan kemampuan pemerintah digitalnya dengan bekerjasama dengan penyedia jasa di bidang siber. Sebagai contohnya, pemerintah sudah menandatangani nota kesepakatan kerjasama dengan Cisco, perusahaan teknologi global, tentang penyelenggaraan program *Country Digital Acceleration* (CDA). Program di Indonesia berfokus pada lima sektor, yaitu pemerintahan digital, industry digital, BUMN digital, inklusi digital dan keamanan siber.[36] Terdapat dua acuan yang menentukan keberhasilan kerja sama tersebut. Pertama, adanya kemampuan keamanan siber di Indonesia yang sejalan dengan adopsi digital, sehingga mampu menghindari pelaku ancaman siber. Kedua, kerja sama dengan pemerintah dalam koordinasi dan pelaksanaan kebijakan keamanan siber nasional.



Perlu ditekankan bahwa, keterlibatan pihak swasta/ privat penyedia jasa tidak dapat diartikan dengan memberikan kuasa terkait kerangka kerja keamanan siber seutuhnya kepada aktor non-pemerintah. Akan tetapi, dengan adanya masukan yang diberikan dari pihak ketiga dengan pengetahuan dan kapasitas yang lebih baik,maka diharapkan dapat

tercipta skema perlindungan terhadap keamanan siber yang lebih mumpuni. Dengan cara ini, BSSN maupun instansi pemerintah lainnya dapat mendapatkan perspektif yang lebih lengkap tentang ancaman dan teknik mitigasi yang efektif. Pada akhirnya, masing-masing sektor tersebut memang memiliki perspektif, teknologi, dan juga priotas yang berbeda.

D. Sektor Akademik

Sektor pendidikan, dalam hal ini adalah perguruan tinggi, merupakan salah satu sektor terpenting dalam kerangka kerja keaman siber. Institusi pendidikan merupakan sektor pembentuk sumber daya manusia (SDM) yang dibutuhkan. BSSN dalam tugasnya menjalankan tugas-tugasnya masih kekurangan SDM yang berkompeten. Terdapat beberapa alasan mengapa BSSN masih kekurangan SDM yang mampu untuk bekerja sesuai dengan tuntutan saat ini. Beberapa diantaranya adalah, pertama, berdasarkan kurikulum pendidikan tinggi di Indonesia, jurusan-jurusan kuliah yang menawarkan pelajaran secara teknis mempelajari ranah siber masih terbatas pada jurusan Ilmu Komputer dan beberapa jurusan dalam Fakultas Teknik. Kedua, terdapat perbedaan kompetensi SDM lulusan perguruan tinggi dengan apa yang sebetulnya dibutuhkan di lapangan kerja.

Maka dari itu, dalam skema kerja sama *multi-stakeholders* di atas, sektor akademik memiliki peranan dasar dan substansial, yaitu mempersiapkan Sumber Daya Manusia yang memiliki kecakapan yang dibutuhkan oleh BSSN maupun industri konsultan keamanan siber lainnya. Maka dari itu, alur kerja sama yang dapat dibentuk adalah, sebagai contoh: BSSN dapat menginformasikan kepada institusi pemerintah yang menangani Pendidikan Tinggi, dalam hal ini adalah Kemenristekdikti mengenai standar, serta jenis kecakapan-kecakapan baru dan khusus yang dibutuhkan dalam konteks penyelenggaraan sistem keamanan siber. Kemenristekdikti kemudian dapat mengatur kurikulum pendidikan sesuai dengan kebutuhan tersebut sehingga perguruan tinggi dapat mengadopsi kurikulum tersebut. Perguruan Tinggi bersama Kemenristekdikti juga dapat mengembangkan jurusan- jurusan atau mata kuliah yang sesuai dengan era digital ini. Di sisi lain, sektor akademik pun dapat memberikan input rekomendasi kebijakan bagi BSSN maupun instansi pemerintah melalui kajian- kajian akademis. Hasil akhir yang diharapkan adalah ketersediaan sumber daya manusia yang cakap dalam bidang-bidang baru yang dibutuhkan dalam konteks keamanan siber serta penguatan struktur dan regulasi yang dihasilkan dari beragam kajian strategis yang berdasar pada nilai-nilai akademis.

Seperti lima sektor lainnya, sebuah standar manajemen keamanan siber juga dibutuhkan oleh industri umum. Pada saat ini, BSSN telah mencetuskan enam sektor kritis yang rawan terkena serangan siber, yaitu: pemerintahan, pertahanan dan keamanan, perbankan, kesehatan, ESDM, transportasi, TIK, dan ketahanan pangan.[40] Maka dari itu, pembahasan akan lebih diutamakan pada pola kerja sama antara keenam industri yang bergerak dibidang tersebut dan BSSN. BSSN sebagai koordinator diharapkan memiliki skema kerja sama tidak hanya dengan instansi pemerintah yang menurusi sektor tersebut, tetapi juga dengan industri non-pemerintah lainnya. Hal ini disebabkan oleh ekosistem siber yang aman membutuhkan sebuah kerja sama yang baik aantara semua pihak dan terkoordinasi.

E. Sektor Industri

Dalam skema kerja sama *multi-stakeholders*, peta koordinasi bermula dari BSSN yang menerapkan standar bagi keamanan siber yang harus dimiliki oleh industri ini. Standar tersebut dapat berupa sistem CERT yang harus dimiliki, kualifikasi SDM yang dibutuhkan, maupun standar teknologi dan sistem informasi yang harus dimiliki oleh perusahaan. Kemudian, BSSN bersama pemerintah dapat mengeluarkan sebuah regulasi hukum yang mengatur mengenai keamanan siber bagi sektor ini. Karena status industrinya yang rawan akan ancaman siber, maka sebuah regulasi hukum sangat diperlukan untuk melindungi industri-industri ini secara legal. Setelah itu, BSSN, pemerintah, dan industri tersebut mensosialisasikan mengenai regulasi tersebut kepada masyarakat, supaya masyarakat juga lebih memahami isu keamanan siber dan berhati- hati.

Hal yang perlu dicermati di sini adalah kerja sama BSSN dengan industri terkait masih minim. Hal ini dapat disebabkan oleh usia BSSN yang masih dini dan juga sedikitnya dokumen atau sumber data digital terpercaya yang membahas mengenai kerja sama BSSN dengan industri tersebut. Tulisan ini baru menemukan tiga sektor industri yang sudah menginisiasi kerja sama dengan BSSN, yaitu sektor perbankan, kesehatan, dan telekomunikasi dan infrormasi. Selain itu, penelitian di bagian ini tidak termasuk sektor pemerintah, yang sudah dibahas di bab sebelumnya.

- **Finansial dan Perbankan**

Dengan meningkatnya digitalisasi kegiatan perbankan dan finansial, data pribadi pengguna jasa perbankan dan finansial menjadi rentan terhadap serangan siber. Maka dari itu, penjaminan keamanan siber sangat mempengaruhi reputasi perusahaan tersebut dan dapat meningkatkan atau mengurangi kepercayaan masyarakat untuk menggunakan jasa perusahaan. Sejauh ini, kerja sama terkait pencegahan serangan siber di sektor perbankan baru dijalin BSSN dengan Bank Rakyat Indonesia (BRI), berupa pengamanan penggunaan *e-cerfiticate*. Terlepas dari kerjasama BSSN dengan BRI, mekanisme pencegahan kejahatan siber yang dimiliki oleh industri perbankan dan finansial di Indonesia hanya terbatas pada penerapan ISO 27001 yang mengatur tentang sistem manajemen keamanan informasi. Beberapa contoh instansi yang telah memiliki sertifikat tersebut adalah Bursa Efek Indonesia (BEI)[41] dan PT Bank Central Asia Tbk (BCA).[42]

Sementara itu, dengan perkembangan teknologi yang semakin pesat, jumlah *fintech* juga semakin meningkat. Namun terdapat perbedaan antara *fintech* yang terdaftar di Otoritas Jasa Keuangan (OJK) yang hanya berjumlah 70 perusahaan dengan jumlah fintech yang terdapat di *playstore* yang berjumlah ratusan.[43] Maka dari itu, *fintech* yang sebenarnya baik untuk mendukung UMKM sering disalahgunakan.

Maka dari itu, sebuah konsep keamanan siber bagi penyedia jasa *fintech* sangat penting. Pertama, keamanan aplikasi, kedua, keamanan penyimpanan awan (*cloud*), dan yang terakhir adalah keamanan terpadu yang bisa mendeteksi segala ancaman.[44] Beberapa *fintech* yang telah mendapatkan ISO 20071 adalah Privyld, Modalku, dan juga Tamasia, sebuah *fintech* syariah yang bergerak dibidang jual beli emas. Menimbang sedikitnya jumlah *fintech* dan perbankan yang telah mendapatkan sertifikat ISO 20071, bisa dikatakan bahwa keamanan siber belum menjadi standar yang diperhatikan. Selain itu, walaupun beberapa *fintech* di atas dudah memiliki ISO 20071, yang berskala internasional, dibutuhkan pula sebuah standar nasional dari BSSN untuk memastikan bahwa *fintech* yang ada di Indonesia seusai dengan keadaan dan kebutuhan masyarakat Indonesia.

- **Kesehatan**

Saat ini semakin banyak rumah sakit, pusat medis, dan fasilitas kesehatan lainnya yang menggunakan teknologi digital untuk catatan dan arsip mereka. Segala hal yang berkaitan dengan pasien atau pengguna layanan jasa kesehatan tersebut disimpan secara *online*. Maka dari itu, sektor kesehatan saat ini menjadi rawan untuk mendapatkan serangan siber. Bagi penjahat dunia maya, informasi ini dapat digunakan untuk mengubah catatan pasien, mendistribusikan kembali atau memalsukan resep atau melakukan kejahatan berbahaya dengan meretas rencana perawatan pasien.

Koordinasi BSSN dengan industri kesehatan saat ini masih mengacu pada kerjasama BSSN dengan Kementerian Kesehatan, berupa penggunaan sertifikat elektronik yang dapat dimanfaatkan dalam sistem pelayanan pulik berupa digital signature dan post border untuk penyederhanaan perizian dan tata niaga ekspor impor bidang alat kesehatan. Sementara itu, ruang lingkup kerja sama iini meliputi: pemanfaatan sertifikat elektronik, pengamanan teknologi

informasi dan komunikasi, peningkatan dan pengembangan sumber daya manusia, pertukaran informasi, dan pemanfaatan lain yang disepakati. Kerja sama antara BSSN dan Kemenkes ini merupakan titik terang bagi standardisasi SDM, teknologi, dan tata kelola dalam industri kesehatan karena Kemenkes membawahi pelaku usaha industry lainnya. Namun demikian, karena MoU kerjasama ini baru saja terjalin, belum ada dokumen tersedia yang dapat menunjukan sampai mana eksekusi kerja sama ini telah berlangsung.

- **Informasi dan Komunikasi**

Khusus pada sektor informasi dan komunikasi, BSSN bekerja sama dengan Kementerian Komunikasi dan Informasi. Pada awalnya, dikhawatirkan terjadi tumpang tindih fungsi antara BSSN dan Kemenkominfo. Dalam sektor ini, isu yang paling meresahkan adalah adanya penyalahgunaan media sosial dalam kehidupan berbangsa dan bernegara. Namun, BSSN menegaskan bahwa tumpang tindih tersebut tidak terjadi karena isu media sosial sampai saat ini masih berada dibawah tanggung jawab Kemenkominfo.[47]

Sementara itu, usaha BSSN dalam mengamankan sistem informasi dan komunikasi sejauh ini diejawantahkan dalam kerja sama perlindungan data berupa penggunaan sertifikat elektronik oleh beberapa instansi seperti yang telah dijabarkan sebelumnya. Sedangkan untuk perusahaan- perusahaan yang bergerak di bidang telekomunikasi dan infromasi, koordinasi dilakukan dengan Kemenkominfo. Di sinilah perlu adanya koordinasi yang lebih aktual antara Kemenkominfo dan BSSN untuk melaksanakan fungsinya masing- masing dan untuk menentukan standar keamanan siber dalam sektor informasi dan komunikasi

F. Komunitas Masyarakat

Dalam skema kerja sama *multi-stakeholders* , komunitas masyarakat siber memegang peranan yang sangat penting karena posisinya yang langsung berada di tengah-tengah masyarakat. Komunitas dalam bidang keamanan siber akan terdiri dari para ahli teknis di bidang keamanan siber, yang bernaung dibawah asosiasi kemasyarakatan atau perkumpulan nirlaba. Peranan komunitas ini umumnya menjadi wadah organisasional tempat para industri dan ahli yang bergerak di bidang ICT berkolektif. Aktor masyarakat ini memiliki peran-peran spesifik yang mampu berkontribusi terhadap strategi kerjasama keamanan siber nasional, khususnya bersama BSSN:

- Komunitas yang memberikan respon teknikal ketika terjadi insiden siber. Inisiasi teknikal ini pada umumnya bersifat global, namun kehadirannya telah ada di tingkat nasional,[48] misal adalah *Computer Emergency Response Team* (CERT) yang dibentuk melalui kesepakatan IETF/ICANN.[49] CERT bisa dibentuk oleh masyarakat maupun pemerintah, seperti GovCSIRT (Pusat Monitoring Penanganan Insiden Keamanan Informasi untuk Instansi Pemerintah) dan ID-SIRTII CC sebagai pusat koordinasi seluruh CERT yang ada di Indonesia. Namun yangdimaksud disini adalah CERT yang spesifik berasal dari inisiatif masyarakat. Indonesia memiliki inisiatif CERT di tingkat masyarakat seperti ID-CERT. ID-CERT mampu berperan sebagai *security advisor*[50] dari sektor masyarakat dan berkontribusi dalam kanal komunikasi dan konsultasi ketika insiden ancaman siber terjadi. BSSN dapat Selain berperan dalam aksi repsonsif, ID-CERT juga memiliki peran di aksi preventif dalam dalam mendiseminasi kesadaran publik tentang urgensi *IT Security* dari pakarnya.
- Komunitas yang memberikan edukasi publik kepada masyarakat terkait isu-isu literasi digital dan keamanan siber. Indonesia memiliki komunitas masyarakat seperti *Indonesia Cyber Security Forum*, Masyarakat Telekomunikasi (Mastel), ICT Watch dan *Indonesia Honeynet Project* yang telah bergiat dalam isu tersebut. Aktor-aktor tersebut juga bertindak sebagai *watchdog* dan memberikan kontribusi perihal analisis kebijakan dan advokasi dalam isu keamanan siber yang tengah menjadi prioritas di masyarakat. Hal ini dapat menjadi peluang kerjasama

dalam strategi keamanan siber nasional. Sebagai seorang ahli, komunitas masyarakat tersebut juga memiliki kapasitas untuk membangun kemampuan teknis sumber daya manusia, baik di sektor pemerintah maupun industri, di bidang keamanan siber. Kerjasama dapat dilakukan antara BSSN dan komunitas-komunitas tersebut di bidang pembangunan kapasitas teknik SDM.

- Komunitas yang menjadi tempat berhimpun dan berjejaring para *stakeholder* di bidang ICT.[51] Inisiatif global yang telah dibentuk adalah Network Operators' Group (NOG). NOG merupakan forum informal yang mempertemukan para profesional di bidang IT, industri, akademisi dan pemerintah untuk mendiskusikan isu terkini dan sebagai platform berbagi pengetahuan bersama. Sangat memungkinkan untuk melibatkan IDNOG dalam kerangka kerjasama strategi keamanan siber. IDNOG mampu memfasilitasi adanya wadah komunikasi *multi-stakeholder* yang nantinya akan bermanfaat bagi eskalasi wacana maupun isu dalam keamanan siber. Forum ini mampu menjadi langkah awal dari koordinasi antar sektoral di bidang keamanan siber.

G. POLRI/TNI

Masuknya POLRI dan TNI dalam skema kerja sama *multi-stakeholders* dikarenakan hanya POLRI yang memiliki kewenangan untuk melakukan penegakan hukum apabila terjadi suatu kejahatan siber, dan juga hanya TNI yang memiliki kewenangan untuk melakukan operasi pengamanan apabila serangan siber tersebut mengancam pertahanan dan kedaulatan negara. Pada tahun 2017 ketika BSSN berdiri, POLRI juga menginisiasi berdirinya Direktorat Siber Bareskrim yang menangani tindak kriminal siber. Maka dari itu, baik BSSN maupun Direktorat Siber merupakan dua instansi yang berusia muda dan ditakutkan terjadi tumpang tindih tugas. Namun, bagian humas POLRI menegaskan bahwa tidak akan terjadi saling rebut fungsi karena Dit Siber akan selalu berkoordinasi dengan BSSN sebelum bareskrim menangani sebuah kasus.[52] Selain itu, POLRI juga bekerja sama dengan komunitas masyarakat dalam identifikasi kasus kejahatan siber karena sampai saat ini, SDM Dit Siber masih terbatas.

Dengan demikian, BSSN yang berkoordinasi dengan POLRI akan mendapatkan informasi teraktual mengenai apa yang sedang terjadi di masyarakat. Koordinasi ini juga merupakan koordinasi dua arah, di mana BSSN dapat melaporkan kepada POLRI apabila terdapat serangan yang teridentifikasi oleh BSSN, sehingga POLRI melalui Bareskrim dapat langsung menindak serangan siber tersebut. Sejauh ini, kerja sama dengan POLRI lebih mengarah pada kampanye hitam menuju Pemilu 2019, yang juga melibatkan Kemenkominfo.

Sementara itu, ancaman siber tidak hanya dapat mengganggu stabilitas keamanan masyarakat, namun juga keamanan negara dan kedaulatannya. Beberapa perdebatan saat ini adalah, dengan meningkatnya kegiatan siber, kemungkinan terjadinya perang siber juga membesar. Bukan tidak mungkin bahwa konsep konflik atau perang tradisional antar negara yang menggunakan senjata api dan juga drone sekarang berganti ke persenjataan yang dampaknya lebih signifikan, yaitu virus, trojan, atau malware. Perdedaan antara perang konvensional dan perang siber adalah salah satunya target penghancuran. Jika target penghancuran perang konvensional adalah infrastruktur, persenjataan dan ekonomi, target perang siber saat ini adalah para pembuat kebijakan, melalui doktrinasi dan juga distraksi terhadap pengambilan kebijakan. Maka dari itu, perang siber lebih berbahaya dibandingkan perang konvensional karena perang ini dapat menghancurkan negara justru dari dalam negara itu sendiri.[53]

Maka dari itu, alur koordinasi antara BSSN dapat terjadi dengan dimulai dari BSSN sebagai koordinator yang memberikan informasi kepada TNI mengenai ancaman serangan siber yang dapat mengganggu keutuhan dan kedaulatan negara. Kemudian keduanya dapat merumuskan respon strategis yang efektif untuk mempertahankan keamanan negara. Sementara itu, kerjasama yang telah dilakukan antara BSSN dan TNI sejauh ini masih berada pada penjaminan keamanan arsip digital TNI oleh BSSN. Sampai saat ini, belum ada MoU yang secara jelas memisahkan tugas dari BSSN, Dit Siber Bareskrim POLRI, dan juga TNI. Pola koordinasi dan kerja sama di antara ketiganya juga belum diformulasikan dengan jelas. Sementara dengan TNI, isu-isu strategis yang dapat dijalankan melalui koordinasi kedua instansi masih berada pada tahap perumusan. BSSN diharapkan mampu bersinergi dengan TNI dan POLRI guna terciptanya koordinasi strategi keamanan siber yang lebih baik di masa mendatang.

RENCANA AKSI STRATEGI KEAMANAN SIBER INDONESIA

Dari penjabaran kerangka koordinasi dan kerjasama dalam strategi keamanan siber Indonesia diatas, dapat disimpulkan sebuah rencana aksi (*action plan*) yang lebih rinci mengenai strategi keamanan siber di Indonesia. Rencana aksi tersebut meliputi tahap **preventif**, **identifikasi**, **respons**, dan **pemulihan** (*recovery*) atas serangan-serangan siber yang mengancam Indonesia. Selain identifikasi tahap, rencana aksi ini juga membatasi adanya tiga subjek yang menjadi fokus dalam implementasi strategi ini yaitu (a) Kepentingan Pemerintah/Kedaulatan Negara (b) Infrastruktur Kritis dan (c) Masyarakat. Pembagian ini menggunakan pendekatan *risk-based* yang terbagi berdasarkan dampak yang akan ditimbulkan terhadap subjek yang berbeda.

Preventif

Kepentingan Pemerintah/ Kedaulatan

Tahap preventif di Pemerintah dapat dimulai dengan penerapan standar protokol keamanan siber untuk instansi pemerintah dan urusan negara lainnya yang terkait dengan kedaulatan. Perlu adanya identifikasi objek rahasia negara dalam ruang siber yang harus mendapatkan perlindungan siber lewat penerapan standar protokol keamanan siber. Dalam *Pedoman Pertahanan Siber* dari Departemen Pertahanan tahun 2014 yang mengacu pada Permenhan No. 82 Tahun 2014, aksi preventif ini termasuk dalam bentuk pertahanan siber.[54]

Tahap preventif di ranah pemerintah dimulai dengan *risk analysis* dalam mengukur kerentanan instansi pemerintah dan data yang dimiliki terhadap ancaman siber. Tindakan seperti *penetration testing* diperlukan untuk menguji sistem perlindungan siber sebuah instansi pemerintah dan meninjau apakah standar protokol keamanan siber sudah dipenuhi atau belum.[55]

Subjek yang dapat melakukan tindakan preventif di ranah kepentingan pemerintah adalah Gov-CSIRT sebagai CERT bentukan pemerintah, dibawah kewenangan Kemkominfo. Kementerian Pertahanan juga memiliki kewenangan dalam mengamankan rahasia negara di ruang siber dan telah menyusun tahap penyelenggaraan pertahanan siber yang termasuk tahap preventif didalamnya. Tujuh tahapan preventif yang menjadi kewenangan Kementerian Pertahanan berfokus lebih banyak pada peningkatan kapasitas arsitektur pengamanan informasi yang bersifat *hardware*.[56] Prioritas fokus yang terlalu condong ke *hardware* juga perlu diimbangi dengan peningkatan kapasitas SDM dan kesadaran individu yang berada di jajaran pemerintah dan pertahanan negara.

Infrastruktur Kritis

Pemerintah Indonesia telah mengidentifikasi sektor-sektor yang termasuk infrastruktur kritis, begitu juga dalam ranah ruang siber. Sektor ini mencakup perbankan, kesehatan, energi, transportasi, TIK dan ketahanan pangan.[57] BSSN juga telah menyinggungnya upaya perlindungan infrastruktur kritis dalam dalam Strategi Keamanan Siber Nasional (SKSN) yang secara internal berfokus pada Pembangunan Sistem dan Pembangunan Kekuatan.[58]

Pembangunan Sistem mencakup pengembangan infrastruktur yang membuka kesempatan pemerintah untuk menjalin relasi dengan dengan pihak swasta sebagai pemilik kepentingan. Pembangunan infrastruktur ini akan mencakup Pusat Pengendalian Siber Nasional dan Jaringan Pertukaran Informasi Nasional. Pembangunan Kekuatan disini adalah koordinasi pemerintah dengan aktor masyarakat profesional seperti jejaringan *white hat hacker* di Indonesia yang tergabung dalam ID-CERT. ID-CERT telah membantu pemerintah untuk menanggulangi krisis-krisis siber di Indonesia. Dukungan pemerintah terhadap masyarakat siber juga akan membantu proliferasi budaya siber yang bertanggung jawab di masyarakat.

BSSN, dibantu oleh Kemkominfo, telah menyiapkan embrio badan khusus yang menangani perlindungan infrastruktur kritis dari tahun 2016 sampai pada tahun 2018 di CIIP-ID Summit 2018, diluncurkan *Critical Infrastructure I Protection Indonesia* yang akan berada di bawah kewenangan BSSN.[59] Dengan adanya CIIP-ID besar peluang Pemerintah Indonesia, khususnya BSSN, sebagai koordinator untuk mampu membangun relasi dan alur koordinasi langsung dengan industri yang menangani sektor infrastruktur kritis ini sebagai tahap preventif dalam strategi keamanan siber untuk memantau kondisi keamanan siber sektor terkait.

Masyarakat

Di tahap preventif serangan siber, penting untuk melibatkan masyarakat dalam subjek yang dilindungi karena masyarakat adalah kelompok yang menjadi target ancaman siber dengan cakupan terluas. Oleh karena itu, usaha preventif terhadap serangan siber yang menargetkan masyarakat harus bersifat *grassroot*. BSSN dan Pemerintah dapat menyebarluaskan literasi keamanan siber dengan bermitra dengan komunitas professional, NGO dan *think-tank* yang berfokus pada peningkatan kesadaran akan budaya siber yang aman, antisipatif, dan preventif.[60]

Identifikasi

Kepentingan Pemerintah/ Kedaulatan

Tahap identifikasi ancaman siber menjadi lanjutan dari proses analisis risiko dari ancaman siber tersebut. Tahapan identifikasi dimulai dengan mendeteksi seberapa besar risiko ancaman siber pada subjek tertentu akan membantu untuk menentukan strategi penanganan yang perlu diambil oleh *stakeholder* yang berwenang. Kementerian Kominfo RI menjadi garda depan dalam tahap identifikasi insiden ancaman siber ini, dibantu dengan komunitas masyarakat seperti ID-CERT.

Sedangkan dalam perlindungan kedaulatan negara, menurut *Pedoman Pertahanan Siber*, tahap identifikasi ini dapat dikerucutkan dalam tindakan analisis serangan, meskipun tahapan dalam keduanya saling bersinggungan dengan tahap respon. Prioritas dalam identifikasi serangan siber adalah mampu melakukan analisa piranti lunak berbahaya dan melakukan investigasi forensik digital.[61]

Infrastruktur Kritis

Peran CSIRT atau CERT menjadi sangat krusial untuk perlindungan sektor-sektor infrastruktur kritis, khususnya dalam mengidentifikasi dan mendeteksi ancaman siber yang mungkin muncul. Dari enam sektor infrastruktur kritis yang termasuk dalam pengklasifikasian BSSN yaitu perbankan, kesehatan, energi, transportasi, TIK dan ketahanan pangan, masing-masing diantaranya berada dibawah kewenangan kementerian tertentu. Peralihan penyimpanan aset informasi dan tingginya tingkat adopsi teknologi di enam sektor tersebut menjadi urgensi diperlukannya mekanisme identifikasi ancaman dan CERT khusus yang menangani isu ancaman siber tersebut. Hanya ada satu institusi pemerintah yang membawahi bidang riset dan teknologi yaitu Badan Pengkajian dan Penerapan Teknologi (BPPT) di Indonesia yang memiliki CSIRT sendiri yang berfungsi untuk mengidentifikasi dan merespon adanya ancaman siber yang mengganggu keamanan informasi dan data penerapan teknologi informasi di Indonesia.[62]

Respon

- **Kepentingan Pemerintah/ Kedaulatan**

  Tahap respon akan terbagi menjadi (1) penindakan teknis ancaman siber dan (2) penindakan hukum tindak ancaman siber. Dalam tahap respon terhadap ancaman siber khususnya di ranah Pemerintah, Indonesia telah memiliki Gov-CSIRT (Government Computer Security Incident Response Team) untuk menangani insiden ancaman siber di instansi pemerintah dan pemerintahan lokal, baik provinsi maupun daerah, di Indonesia. Kewenangan untuk menindak kejahatan yang mampu mengancam kedaulatan negara seperti peretasan internasional diserahkan kepada Satuan Siber TNI, Pusat pertahanan Siber Kementerian Pertahanan RI dan Badan Intelijen Negara.

- **Infrastruktur Kritis**

  CSIRT/CERT Sektoral masih berperan vital dalam memberikan respon ketika ancaman terjadi. Penindakan teknis dari perusahaan industri tertentu atas sebuah insiden telah menjadi protokol standar untuk menangani ancaman siber. CSIRT/CERT Sektoral dapat menjadi medium koordinasi antar asosiasi perusahaan dalam industri tertentu, misal industri energi, dengan asumsi awal bahwa sebuah ancaman siber terhadap satu perusahaan dalam sektor industri menjadi masalah bersama perusahaan lain dalam industri yang sama. Pola ancaman siber dan target yang dicari oleh para peretas bisa dipelajari sebagai lesson learned untuk menentukan best practice lainnya yang bisa dilakukan oleh industri lainnya.

Namun, sebelum pemberikan tindakan teknis, CSIRT/CERT Sektoral perlu menentukan kerangka kerja di setiap sektor terkait tahapan respon yang akan menjadi wewenang CSIRT/CERT Sektoral sesuai dengan isu bersama yang dihadapi dalam sektor tertentu. Ancaman terhadap cyberphysical security yang rentan dalam perangkat IoT yang menjadi adopsi teknologi utama dalam infrastruktur kritis perlu menjadi salah satu prioritas perlindungan. Hal ini dikarenakan kerentanan perangkat IoT cyberphysical security dan berpotensi menjadi salah satu celah peretas dapat mengambil alih kontrol atas informasi dan aset infrastruktur kritis.

- Masyarakat

Penegakan hukum di Indonesia terutama mengenai kejahatan siber yang menimpa masyarakat ditangani oleh Kepolisian RI. Namun, Polri masih memiliki kendala yang berat dalam melaksanakan fungsinya untuk menangkap pelaku kejahatan siber. Di samping pembagian tugas yang belum jelas dengan TNI dan BSSN, Polri juga masih mengandalkan bantuan pihak swasta dan akademik yang memiliki kemampuan teknis dan kapasitas yang lebih mumpuni dari Polri. Penangkapan pelaku pun hanya bisa dilakukan kepada pelaku-pelaku domestik. Sifat kejahatan siber yang trans-border dan anonim membuat ranah siber menajdi sulit disentuh oleh hukum.

Recovery (Pemulihan)

- **Kepentingan Pemerintah/ Kedaulatan**

Pemulihan sektor pemerintah berdasar pada ancaman siber dan persiapan rencana kontingensi kebencanaan. Meskipun telah bersiap dari tahapan pencegahan, tahapan pemulihan perlu memiliki intensitas fokus yang sama dengan tahapan lainnya mengingat ancaman dan kerentatan siber adalah hal yang tidak dapat dihindari. Menyiapkan tahap pemulihan yang efektif dan efisien secara diperlukan untuk meminimalisir kerugian yang ditimbulkan oleh serangan siber, baik terhadap instansi pemerintah tersebut maupun konstituennya.

- **Kepentingan Pemerintah/ Kedaulatan**

Pelaku perusahaan industri infrastruktur kritis dapat menggunakan jasa perusahaan asuransi yang menyediakan asuransi siber seperti *Cyber Enterprise Risk Management*.[66] BSSN dapat menerapkan kebijakan wajib mengasuransikan aset infrastruktur kritis dari ancaman siber sehingga ketika masa pemulihan pasca ancaman siber, para perusahaan yang berada dalam sektor infrastruktur kritis memiliki kesiapan lebih.

- **Kepentingan Pemerintah/ Kedaulatan**

Ketika masyarakat menjadi korban serangan siber, aset, data maupun informasi digital yang menjadi target serangan siber belum tentu sepenuhnya akan bisa mendapatkan proses pemulihan, terlebih apabila hal itu menyangkut kerugian material dan fisik. Hal ini akan berkaitan dengan tahap respon dalam tindak hukum. BSSN maupun Polri belum memiliki kerangka yang menyeluruh terkait pemulihan kasus serangan siber yang menimpa masyarakat. Perlu adanya perlindungan terhadap konsumen atau pengguna masyarakat dalam platform digital dalam prosedur pemulihan.

Rekomendasi rencana aksi secara lebih detail dan spesifik, menyangkut tahapan serta ranah penanganannya digambarkan dalam bagan berikut:

Tahapan	Ranah Penanganan		
	Kepentingan Pemerintah/ Kedaulatan Negara	Infrastruktur Kritis mencakup	Masyarakat Publik
Preventif	Penerapan standar protokol keamanan siber untuk instansi pemerintah dan urusan negara lainnya yang terkait dengan kedaulatan dan *risk analysis* dalam mengukur kerentanan instansi pemerintah dan data yang dimiliki terhadap ancaman siber oleh Gov-CSIRT dan Kementerian Pertahanan.	Pembangunan sistem dan kekuatan infrastruktur keamanan siber lewat Kemkominfo, ID-CERT dan CIIP-ID.	Penyebaran literasi keamanan siber di masyarakat secara luas.
Identifikasi	Mendeteksi seberapa besar risiko ancaman siber pada subjek tertentu akan membantu untuk menentukan strategi penanganan yang perlu diambil oleh *stakeholder* yang berwenang dan analisis piranti lunak berbahaya dan melakukan investigasi forensik digital.	Identifikasi ancaman siber sektoral melalui CSIRT/CERT Sektoral.	

Tahapan	Ranah Penanganan		
	Kepentingan Pemerintah/ Kedaulatan Negara	Infrastruktur Kritis mencakup	Masyarakat Publik
Respons	Penindakan teknis ancaman siber oleh Gov-CSIRT dan (2) penindakan hukum tindak ancaman siber oleh BIN, Pushansiber Kemhan RI dan Satuan Siber TNI.	CSIRT/CERT Sektoral menjadi medium koordinasi antar perusahaan dalam tiap sektor industri infrastruktur kritis, fokus pada mempelajari hal-hal sebelumnya dan menentukan penanganan terbaik ketika insiden terjadi.	Penegakan hukum dilakukukan oleh POLRI terkait tindak kriminal siber yang menyasar masyarakat luas.
Pemulihan	Pemulihan sektor pemerintah berdasar pada ancaman siber dan persiapan rencana kontingensi kebencanaan untuk meminimalisir dampak serangan siber pada instansi dan konstituennya.	Asuransi terhadap aset infrastruktur kritis dari serangan siber, bermitra dengan pihak swasta penyedia jasa.	Mekanisme perlindungan pengguna dalam *platform* digital ketika terjadi serangan siber.

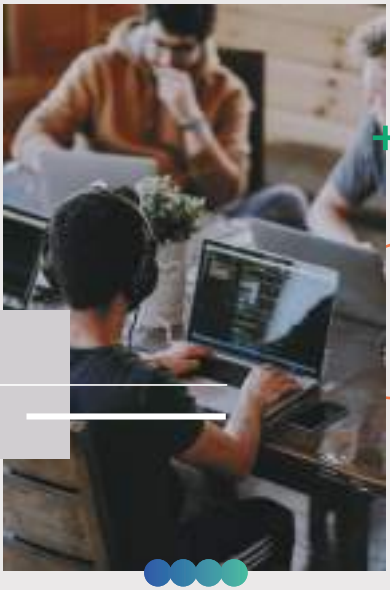
KESIMPULAN

Keamanan siber merupakan salah satu bentuk ancaman non-tradisional baru bagi pertahanan dan keamanan negara yang sudah sepatutnya mendapatkan perhatian besar dari pemerintah maupun berbagai sektor terkait di dalam negara. Natur ranah siber yang tidak lagi berbataskan pada teritori menjadikan ancaman yang terjadi di dalamnya dapat teramplifikasi dengan lebih besar ketika tersebar melalui jaringan-jaringan yang saling terhubung di dalam internet. Ancaman tersebut pun dapat pula timbul dan dimanfaatkan dari kelemahan keamanan dari individu yang dieksploitasi oleh penyerang. Oleh karena itu, diperlukan kebijakan terkait keamanan siber yang bersifat menyeluruh dan melingkupi seluruh aspek pemerintah dan kenegaraan hingga mencapai level individu warga negara.

Pendirian Badan Siber dan Sandi Negara (BSSN) oleh pemerintah Indonesia diharapkan mampu memperkuat lansekap keamanan siber Indonesia secara organisasional/institusional. Keberadaan institusi ini diproyeksikan dapat memberikan standar baru yang lebih baik untuk penciptaan strategi keamanan siber di Indonesia. Fungsi koordinasi dari BSSN dilihat sebagai sebuah fungsi vital yang diharapkan dapat menjembatani hambatan-hambatan birokrasi terkait koordinasi antarlembaga maupun antarsektor yang seringkali menghalangi terciptanya harmonisasi kebijakan. Selain itu, BSSN juga diharapkan dapat memberikan kerangka regulasi legal yang lebih jelas terkait strategi keamanan siber di Indonesia.

Berangkat dari hal tersebut, dirumuskan skema rekomendasi alur koordinasi yang dapat dijadikan acuan bagi BSSN dalam menjalankan fungsinya tersebut. Alur koordinasi tersebut disusun dengan mempertimbangkan adanya potensi kerjasama maupun benturan yang dapat terbentuk dengan adanya silang kepentingan ataupun ranah kerja. Dalam pelaksanaannya, skema alur koordinasi ini kemudian juga diharapkan untuk dapat merujuk kepada rencana aksi terkait pelaksanaan strategi keamanan siber Indonesia. Dalam kerangka strategi keamanan siber nasional, keamanan dan pertahanan negara menjadi unsur *referent object* yang paling penting dan utama. Namun, unsur-unsur pembentuk terciptanya keamanan siber nasional ini pun tidak terlepas dari pengamanan terhadap objek lainnya seperti infrastruktur kritis dan juga keamanan jaringan dari individu.

Untuk itu, kerjasama *multistakeholders* yang harmonis dan terkoordinasi antara pemerintah, kelompok bisnis, akademisi, dan komunitas masyarakat menjadi syarat mutlak bagi tercapainya tujuan utama keamanan siber nasional Indonesia. Koordinasi antarinstitusi dan antarsektor di bawah payung BSSN diharapkan dapat menghindarkan dari kemungkinan terjadinya tumpang tindih kepentingan maupun cakupan lingkup kerja. Kesemuanya kemudian dapat mendukung terciptanya ekosistem keamanan siber nasional yang lebih komprehensif.



REFERENSI

[1]International Telecommunication Union (ITU). (2009). Understanding Cybercrime: A guide for Developing Countries. [daring] Tersedia di: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [Diakses pada 31 Dec. 2018].

[2]Ibid.

[3]Ibid.

[4]Pemaparan Kombes Bareskrim Polri Ricky, pada Convention of Cybersecurity 2018.

[5]Ibid.

[6]Ibid.

[7]Ibid.

[8]Moran, A. (2015). Intelligence and security. In: P. Hough, S. Malik, A. Moran and B. Pilbeam, ed., International Security Studies: Theory and Practices, 1st ed. New York: Routledge, p.178.

[9]Tirtapradja, W. (2018). Data Classification and Cloud Computing: UK National Healthcare System's Attempt to Improve Cybersecurity. CfDS Case Study, 38, hal.1.

[10]BSSN (2018). PRESS RELEASE BSSN AMANKAN SISTEM ELEKTRONIK MILIK KEMENKES. [daring] Tersedia di: https://bssn.go.id/wp-content/uploads/2018/10/29102018-PRESS-RELEASE-MoU-BSSN-KEMENKES.pdf [Diakses pada 3 Jan. 2019].

[11]Rilis Survei APJII (Asosiasi Penyedia Jasa Internet Indonesia) tahun 2017 tentang penetrasi pengguna internet dan profil pengguna internet. Diakses di laman https://apjii.or.id/survei

[12]2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law diakses di laman https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

[13]Norton, 2017 Norton Cyber Security Insights Global Report, Diakses di laman https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[14]Artikel dari Tempo.Co, 2018 Microsoft: Kejahatan Cyber di Indonesia Rugikan Rp 33,29 Miliar https://bisnis.tempo.co/read/770935/microsoft-kejahatan-cyber-di-indonesia-rugikan-rp-3329-miliar/full&view=ok

[15]Nugraha, Leonardus dan Putri, Dinita (2016), Mapping the Cyber Policy Landscape: Indonesia, gp digital.org https://www.gp-digital.org/wp-ontent/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf hal. 9

[16]Hasil penilaian Global Security Index tahun 2017 yang dilakukan ITU diakses di laman https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[17]Rilis hasil penilaian National Cyber Security Index 2018 diakses di laman https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

[18]Regulasi yang tertuang dalam Peraturan Presiden 53 tahun 2017 diakses di laman https://jdih.bssn.go.id/wp-content/uploads/2017/06/Perpres_Nomor_53_Tahun_2017-1Signed.pdf

[19]Regulasi yang tertuang dalam UU nomor 36 tahun 1999 diakses di laman https://ppidkemkominfo.files.wordpress.com/2012/11/uu-no-36-tahun-1999-tentang-telekomuniksi.pdf

[20]Regulasi yang tertuang dalam UU nomor 11 tahun 2008 diakses di laman https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[21]Regulasi yang tertuang dalam UU nomor 19 tahun 2016 diakses di laman https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf

[22]Regulasi yang tertuang dalam PP nomor 82 tahun 2012 diakses di laman https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

[23]UU Pertahanan dan Keamanan Siber menjadi Rancangan undang-undang yang dibahas dan akan diundangkan di tahun 2019 diakses di laman http://www.dpr.go.id/uu/prolegnas

[24]Informasi mengenai ISO/IEC 27301 tentang Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity secara detail dan singkat dapat diakses di laman https://www.iso.org/standard/44374.html

[25]Putra, Y.M. (2018). BSSN: Ahli Keamanan Siber Masih Minim. Republika [daring]. Tersedia di: https://trendtek.republika.co.id/berita/trendtek/internet/18/04/06/p6rppn284-bssn-ahli-keamanan-siber-masih-minim. (Diakses pada 5 Januari 2019)

[26]Islami, M.(2017).Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. Puslitbang Aptika dan IKP Kemenkominfo.[daring]. Tersedia di: https://media.neliti.com/media/publications/233807-tantangan-dalam-implementasi-strategi-ke-d162ca8b.pdf (Diakses pada 6 Januari 2019)

[27]Sutedja, Ardi (n.d) Peran "Multi-Stakeholder" Di Dalam Mendukung Keamanan & Ketahanan Siber Nasional, Dipresentasikan sebagai materi dari Convention on Cybersecurity 2018.

[28]Chaerudin, A. (2018). Strategi Keamanan Siber Nasional. [daring]. Tersedia di https://bssn.go.id/wp-content/uploads/2018/08/Strategi-Keamanan-Siber-Nasional-signed.pdf. (Diakses pada 4 Januari 2019)

[29]Islami,M. (2017)

[30]SINDO News. (2018). Pembentukan BSSN dan Ancaman Siber [daring].https://nasional.sindonews.com/read/1271782/18/pembentukan-bssn-dan-ancaman-siber-1515352267/13. (Diakses pada 6 Januari 2018)

[31]Germano, J.(2014).Cybersecurity Partnership: A New-Era of Public-Private Collaboration. The center on Law and Security NYU, 2014

[32]Ibid.,2.

[33]Indrajit, R. CERT.CSIRT.ID-SIRTII Tim Pengawas Keamanan Internet.(daring). https://idsirtii.or.id/doc/IDSIRTII-Artikel_CERT.pdf , hal.10

[34]Kementerian Pertahanan. https://www.kemhan.go.id/pusdatin/faq, (diakses pada 6 Januari 2019)

[35]Sokanu.What does an IT consultants do?.(daring). https://www.sokanu.com/careers/it-security-consultant/, (Diakses pada 4 Januari 2019).

[36]Bachdar,S.(2018).Digitalisasi Indonesia Ada di Tangan Cisco.(daring). http://marketeers.com/digitalisasi-indonesia-ada-di-tangan-cisco/. (Diakses pada 5 Januari 2019)

Dikutip dari materi presentasi Pudja Unggul Kartiman dan Arief Santoso, Cisco Systems Indonesia, pada Convention on Cybersecurity, CfDS FISIPOL UGM, 7 Desember 2018.

[38]Manggala,Y.(2018). BSSN: Ahli Keamanan Siber Masih Minim.(Daring). Tersedia di: https://www.republika.co.id/berita/trendtek/internet/18/04/06/p6rppn284-bssn-ahli-keamanan-siber-masih-minim .Republika.co.(Diakses pada 31 Desember 2018)

[39]Dikutip dari materi presentasi Dr. I Made Wiryana, Dosen pada Convention on Cybersecurity 2018, CfDS FISIPOL UGM, 7 Desember 2018.

[40]Ibid.,

[41]Putra, D. (2018). BEI Raih Sertifikat ISO,(daring), http://infobanknews.com/bei-raih-sertifikat-iso/ , (Diakses pada 5 Januari 2019)

[42]Republika.(2016). Penerapan ISO 20071:2013 dapat meningkatkan kepercayaan masyarakat. 2016. https://www.republika.co.id/berita/ekonomi/korporasi/16/09/09/od6u26368-penerapan-iso-270012013-dapat-tingkatkan-kepercayaan-nasabah, (Diakses pada 5 Januari 2019)

[43]Diambil dari presentasi Kombes Pol. Rickinaldo Chaerul, S.I.K., Subdit II Tipidsiber Bareskrim POLRI, pada Convention on Cybersecurity, CfDS FISIPOL UGM, Pada 7 Desember 2019

[44]CNN Indonesia.(2018).Abaikan Keamanan Siber, Bank & Fintech Sasaran Empuk Peretas.(daring) . https://www.cnnindonesia.com/teknologi/20180530192225-185-302344/abaikan-kemanan-siber-bank-fintech-sasaran-empuk-peretas . (Diakses pada 6 Januari 2019)

[45]BSSN. (2018) BSSN Amankan Sistem Informasi Kemenkes. (daring) https://bssn.go.id/wp-content/uploads/2018/10/29102018-PRESS-RELEASE-MoU-BSSN-KEMENKES.pdf (Diakses pada 6 Januari 2019)

[46]Ibid.,

[47]Ferrisa, W. (2018) Kepala BSSn: Media Sosial Urusan Kemkominfo.(daring) https://kominfo.go.id/content/detail/12315/kepala-bssn-media-sosial-urusan-kemkominfo/0/sorotan_media (Diakses pada 6 Januari 2019)

[48]University College London. (2017). International Cooperation Between CERTS:Technical Diplomacy for Cybersecurity International Workshop 38, UNIGF, Geneva. ucl.ac.uk [Daring] Tersedia di https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/images/international-cooperation-between-certs-transcript Diakses pada 7 Januari 2019

[49]Alkazimy, Ahmad. (2017) Peranan ID-CERT dalam penanganan insiden siber di Indonesia. Halaman 2. OWASP Foundation [Daring] Tersedia di https://www.owasp.org/images/f/f0/ID-CERT-OWASP-04032017.pdf Diakses pada 7 Januari 2019

[50]Ibid.,27.

[51]APNIC, n.d, Supporting Network Operator Groups. apnic.net [Daring] Tersedia di https://www.apnic.net/community/support/network-operator-groups/ Diakses pada 8 Januari 2019

[52]KumparanNews.(2018).Polri Pastian Tugas SIber Bareskrim Tak Tumpang Tindih dengan BSSN. (daring) https://kumparan.com/@kumparannews/polri-pastikan-tugas-siber-bareskrim-tak-tumpang-tindih-dengan-bssn. (Diakses pada 7 Januari 2018)

[53]Dikutip dari presentasi Kombes Pol Rickynaldo Chaerul, S.I.K.

[54]Kementerian Pertahanan RI (2014) Pedoman Pertahanan Siber [Daring] kemhan.go.id Tersedia di https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf Diakses pada 9 Januari 2019

[55]Sumari, Arwin (2016) Sentralisasi Mitigasi Cyberattack di Indonesia [Daring] APJIII Tersedia di Diakses pada 10 Januari 2019

[56]Kementerian Pertahanan RI (2014) Pedoman Pertahanan Siber [Daring] kemhan.go.id Tersedia di https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf, Halaman 39. Diakses pada 9 Januari 2019

[57]Chairuddin, Asep (2018) Strategi Keamanan Siber Nasional. [Daring] bssn.go.id Tersedia di https://bssn.go.id/wp-content/uploads/2018/08/Strategi-Keamanan-Siber-Nasional-signed.pdf Diakses pada 3 Januari 2019

[58]Ibid

[59]Kominfo (2018) Perkuat Pertahanan Siber Kominfo Bentuk CIIP ICT Sector https://kominfo.go.id/content/detail/14509/perkuat-pertahanan-siber-kominfo-bentuk-ciip-ict-sector/0/berita_satker Diakses pada 13 Januari 2019

[60]Sutedja, Ardi (n.d) Peran "Multi-Stakeholder" Di Dalam MendukungKeamanan & Ketahanan Siber Nasional, Dipresentasikan sebagai materi dari Convention on Cybersecurity 2018.

[61]Kementerian Pertahanan RI (2014) Pedoman Pertahanan Siber [Daring] kemhan.go.id Tersedia di https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf Halaman 40, Diakses pada 9 Januari 2019

[62]BPPT Indonesia (n.d) Visi dan Misi [Daring] Tersedia di http://csirt.bppt.go.id/profil/visi-dan-misi/ Diakses pada 14 Januari 2019

[63]Ibid.

[64]NEC (2016) Social Value Creation Report: New threats to Critical Infrastructures, Halaman 6 [Daring] Tersedia di https://www.nec.com/en/global/about/vision/report/pdf/SocialValueCreationReport_en_Vol.1.pdf Diakses pada 14 Januari 2019

[65]Lohrmann, Dan (2017) How to Recover from Cyber Incidents in Government [Daring] govtech.com Tersedia di http://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-recover-from-cyber-incidents-in-government.html Diakses pada 14 Januari 2019

[66]CHUBB (2018) Cyber Enterprise Risk Management Insurance [Daring] chubb.com Tersedia di https://www.chubb.com/id-id/_assets/documents/ringkasan-produk--cyber-enterprise-risk-management.pdf Diakses pada 14 Januari 2019

ABOUT CFDS

Center for Digital Society (CfDS) is the research center established by the Faculty of Social and Political Sciences, Universitas Gadjah Mada. The institution is created under the concern over the contemporary dynamics of socio-political condition of the world that is accentuated by the impeccable influence of information technology. The phenomenon triggers the new patterns and complexities in the society, and thus requires new approaches in managing such complexities.

CfDS pledged to delve more on the study of contemporary digital society, including related issues surrounding the topic; such as the issues of smart city and urban development. The emphasis is then put on the utilization of technology to shape the society in becoming digitalized, as well as to bring solvency to social issues.

Vision

Solving Social Problem and Accelerating Prosperity through Indonesia Digital Society

Activities

1. Research and Development
2. Dissemination and Publication
3. Education and Policy Advocacy

Research Scopes

1. Digital Governance
2. Digital Economy
3. Future Technology

facebook.com/cfdsugm
@cfds_ugm
Center for Digital Society (CfDS)
@cfds_ugm
cfds.fisipol.ugm.ac.id
cfds_ugm
CfDS UGM