KEBIJAKAN CYBERSECURITY DALAM PERSPEKTIF MULTISTAKEHOLDER

SERI LITERASI DIGITAL

Editor: Donny B.U.

Mitra penyusun (urut abjad):
Penanggung jawab: **Indriyatno Banyumurti**
Editor: **Donny BU**
Tim: **Deni Ahmad, Dinita Andriani Putri, Hari Styawan, Leonardus K. Nugraha, Merry Magdalena**

ISBN: 978-602-51324-0-7

DAFTAR ISI

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

Kata Pengantar

Menteri Komunikasi dan Informatika Republik Indonesia

untuk buku "**Seri Literasi Digital**"

Assalamu 'alaikum warahmatullahi wabarakatuh,

Salam sejahtera bagi kita sekalian,

Internet adalah produk kebudayaan, dan sudah semestinya Internet digunakan manusia untuk menghasilkan kehidupan yang berbudaya. Namun bak pisau bermata dua, Internet sejatinya hanyalah alat yang dapat memberikan dampak positif maupun negatif tergantung pada cara dan tujuan penggunaannya. Dalam era digital saat ini, beragam informasi semakin merasuk hingga ke gawai setiap orang, baik diharapkan ataupun tidak. Kemampuan individu memilah dan memilih informasi, lantas menjadi hal yang mendesak.

Untuk itulah Literasi Digital menjadi kian signifikan relevansinya, tidak hanya sebagai komplementer, tetapi sebagai program prioritas bersama dalam kerangka melakukan upaya edukasi dan advokasi pengguna Internet. Literasi Digital menurut UNESCO adalah, "*kemampuan menggunakan teknologi informasi dan komunikasi (TIK) untuk menemukan, mengevaluasi, memanfaatkan, membuat dan mengkomunikasikan konten atau informasi, dengan kecakapan kognitif, etika, sosial emosional dan aspek teknis atau teknologi*".

Di sisi lain International Telecommunication Union (ITU) menekankan perlu adanya perhatian khusus terhadap generasi muda yang telah akrab dengan dunia digital, atau dikenal sebagai *digital native*, yaitu mereka yang lahir setelah tahun 1980. ITU pun merekomendasikan bahwa memahami cara generasi *digital native* belajar, bermain dan bahkan melibatkan diri mereka ke tengah masyarakat akan dapat membantu dalam menyusun dan merencanakan

masa depan mereka. Di Indonesia sendiri, lebih kurang 50% total pengguna Internet Indonesia adalah *digital native*.

Dengan demikian, dalam koridor tata kelola Internet (*Internet Governance*), sudah dirasa perlu ada upaya bersama para pemangku kepentingan majemuk (*multistakeholder*) dalam memberikan panduan, arahan ataupun petunjuk agar pengguna Internet dapat mengoptimalkan dampak positif Internet sekaligus meminimalisir dampak negatifnya.

Setelah sebelumnya *multistakeholder* Indonesia menginisiasi adanya Gerakan Nasional Literasi Digital SIBERKREASI, maka kini Kementerian Komunikasi dan Informatika (Kominfo) pun menyambut gembira keberadaan sejumlah buku "Seri Literasi Digital" ini. Kami yakin kerja bersama ini merupakan tahapan penting dan contoh kerja bersama bagi masyarakat informasi di dunia tentang ikhtiar dan upaya membangun Internet yang lebih bermanfaat dan berbudaya.

Untuk itu, apresiasi dan terimakasih saya sampaikan untuk segala pihak yang telah membuat buku seri literasi digital ini hadir di hadapan para pembaca

Wassalamu alaikum warahmatullahi wabarakatuh.

Jakarta, 31 Januari 2018

Menteri Komunikasi dan Informatika Republik Indonesia

Rudiantara

BAB I

Memahami Cybersecurity

Cybersecurity merupakan sebuah istilah yang masih diperdebatkan dan memiliki beragam makna. Pemahaman terhadap apa itu cybersecurity adalah langkah pertama yang penting sebelum melakukan pelibatan yang efektif.

A. **Mendefinisikan Cybersecurity**

Definisi konvensional cybersecurity yang dapat ditemukan di berbagai strategi pemerintah maupun buku panduan perusahaan adalah sesuatu yang terkait dengan perlindungan informasi yang terdapat di dalam lingkungan digital dari penyusupan, akuisisi maupun eksploitasi tanpa izin.

Meskipun demikian, cybersecurity telah memiliki makna yang jauh lebih luas. Pemerintah, lembaga, media dan masyarakat sipil sama-sama menggunakan istilah ini untuk merujuk berbagai hal dalam konteks yang lebih luas. Hal-hal di bawah ini dapat dianggap sebagai beberapa contoh isu dalam cybersecurity:

- Suatu serangan phishing menyebabkan jebolnya data log-in akun bank banyak orang;
- Kelemahan piranti lunak yang membuat private key server, cookies serta password pengguna mudah dijebol;
- Sistem keamanan informasi rumah sakit yang lemah dan menghambat akses data pasien;
- Malware yang menyebabkan padamnya lampu di satu kota;
- Kelompok teroris merencanakan serangan melalui jaringan tersembunyi;
- Pasokan air suatu kota menjadi tidak aman ketika seorang hacker mengambil alih kendali secara remote dari sebuah instalasi air;
- Sebuah video yang melanggar hak cipta diunggah ke sebuah website;
- Suatu jaringan pengedar narkoba menggunakan crypto-currency untuk memperdagangkan narkotika ilegal;
- Sebuah komentar yang menghina seorang pemimpin politik diposting di suatu jaringan sosial media.

Istilah cybersecurity juga dapat dijadikan alasan untuk menerapkan kebijakan yang dapat melanggar hak asasi manusia (HAM). Misalnya, cybersecurity seringkali digunakan oleh sejumlah negara untuk membenarkan pembatasan browsing internet secara tidak transparan dan akuntabel, melarang penggunaan aplikasi anonimitas dan layanan enkripsi, serta memperluas kewenangan aparat penegak hukum untuk melakukan pengintaian tanpa berpedoman pada kebijakan dan tata laksana yang memadai, proporsional, dan profesional.

Cybersecurity

Mengingat masih belum adanya definisi bersama, maka pengertian tentang cybersecurity bergantung pada siapa yang membuat definisi tersebut. Suatu tindakan yang dalam suatu konteks dipahami sebagai pembicaraan yang dilindungi undang-undang (UU), dalam konteks lain (misalnya penghinaan terhadap seorang politisi) dapat dengan mudah dikatakan sebagai cybercrime karena definisi yang ambigu. Oleh karena itu, bisa jadi pertanyaan yang lebih relevan adalah: siapa yang memutuskan apa yang termasuk dan tidak termasuk cybersecurity? Di mana hal tersebut diputuskan?

Dibandingkan dengan berbagai isu kebijakan lain yang dapat berdampak pada HAM, cybersecurity menghadapi tantangan konseptual yang berbeda. Hal ini antara lain disebabkan dari sifat “keamanan” (security) itu sendiri. Keamanan tidak akan pernah dapat dicapai seratus persen atau secara sempurna. Karena itu, cybersecurity masih berada pada posisi yang terus berubah dan dapat dibentuk dan dibangun oleh pengampu kebijakan majemuk (multistakeholder).

Keberagaman multistakeholder yang terlibat dalam cybersecurity juga memberikan tantangan tersendiri. Ini merupakan isu bagi pemerintah, lembaga antar pemerintah, komunitas teknis dan akademisi, sektor swasta serta masyarakat sipil. Dengan belum adanya definisi yang ajeg, istilah cybersecurity ini menjadi amat luas, dan digunakan untuk merujuk hal seperti serangan siber (cyberattack) hingga spam, dan bahkan standar teknis sistem pemungutan suara (voting).

B. Pentingnya Cybersecurity

Jika kita memandang keamanan sebagai kebebasan dari bahaya atau ancaman, salah satu pendorong terpenting dalam pembuatan kebijakan cybersecurity adalah bagaimana ancaman dipahami dalam cyberspace. Tanpa upaya cybersecurity yang tepat, kemungkinan ancaman akan meningkat. Secara umum ancaman dipandang mencakup hal-hal berikut:

- Pencurian data untuk keuntungan komersial, seperti pencurian nomor kartu kredit, atau pencurian data pribadi untuk digunakan untuk spamming atau pencurian identitas;
- Akses kepada data untuk kepentingan mata-mata industri demi mendapatkan keunggulan kompetitif;
- Pencurian data untuk menghancurkan nama baik, atau mendiskreditkan pemerintah atau suatu entitas bisnis, serta mendiskreditkan orang atau sekelompok orang;
- Mengakses data untuk mengumpulkan data intelijen yang dilakukan oleh negara asing maupun entitas non-negara;
- Pengubahan atau penghapusan data untuk alasan komersial, politik, maupun ekonomi;
- Kehilangan kendali atas jaringan akibat serangan yang dirancang untuk melemahkan atau melumpuhkan pemerintah atau suatu perusahaan;
- Manipulasi perilaku pengguna dengan cara memancing pengguna mengunduh (download) malware atau tanpa sengaja melakukan tindakan membahayakan diri lainnya;
- Ancaman kepada karyawan atau publik dengan melakukan serangan siber untuk melumpuhkan fungsi lembaga publik tertentu.

C. **Upaya Cybersecurity**

Meskipun masih belum ada kesepakatan tentang istilah yang digunakan dan isu yang akan dihadapi, sejumlah upaya telah dilakukan selama ini untuk mengatasi ancaman-ancaman yang disebutkan di atas, yang mencakup antara lain:

- Upaya teknis untuk meningkatkan keamanan peragkat keras (hardware) dan piranti lunak (software) yang mencakup sistem dan jaringan informasi. Hal ini dilakukan antara lain dengan menguji sistem yang bersangkutan dengan standar teknis yang ada seperti teknik kriptografi, manajemen identitas dan akses, manajemen risiko rantai pasokan serta jaminan atas kehandalaan software;
- Upaya hukum juga memainkan peranan dalam mengatur persyaratan untuk mendapatkan, menyimpan, memproses serta membagi informasi pribadi oleh lembaga swasta maupun publik. Upaya hukum yang relevan mencakup hukum perlindungan data;
- Upaya terkait proses yang mencakup prosedur, panduan, keputusan institusi dan materi pendidikan yang dirancang untuk meminimalkan peran orang – yang terpisah dari komputer – dalam menciptakan atau memfasilitasi gangguan cyber seperti melalui serangan rekayasa sosial maupun kebiasaaan penggunaan password yang lemah.

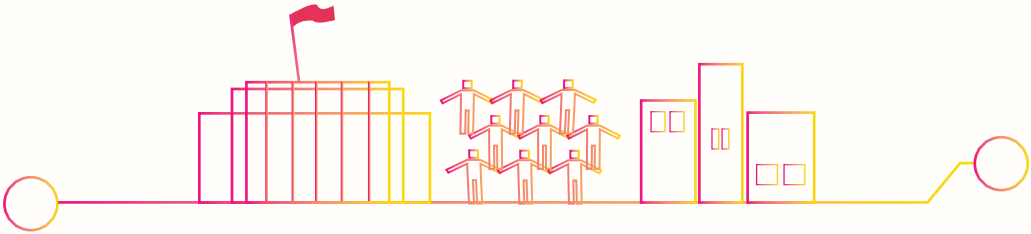
D. **Dimensi Kebijakan Cybersecurity**

Kita baru saja menjelajahi asal usul istilah cyber, serta penggunaan istilah cybersecurity yang begitu luas, ancaman terkait cybersecurity yang mempengaruhi pembuatan kebijakan, serta upaya yang diambil untuk menghadapi ancaman-ancaman tersebut. Sekarang kita akan melihat bagaimana proses pembuatan kebijakan cybersecurity dilaksanakan.

Untuk menjawab pertanyaan ini, kita perlu mengelompokkan beberapa hal, meskipun dalam isu kompleks seperti cybersecurity, tidak ada cara yang pasti atau terbaik dalam melakukannya. Meskipun masih ada sedikit tumpang tindih dalam proses pengelompokan ini, setidaknya ketiga kategori di bawah dapat menjadi pintu masuk dalam memahami pembuatan kebijakan cybersecurity yang berlangsung saat ini:

- Keamanan informasi: pengembangan standar dan proses teknis dan hukum yang dirancang untuk mencegah akses informasi dan jaringan komunikasi tanpa izin;
- Cybercrime: upaya yang dirancang untuk mendeteksi, mencegah dan menyelidiki kegiatan ilegal. Hal ini mencakup kejahatan online maupun kejahatan offline yang memiliki unsur online. Legislasi cybercrime, upaya pengawasan digital dan pembatasan konten online masuk ke dalam wilayah ini;
- Cyber conflict: undang-undang dan kebijakan yang ditujukan untuk mengelola, membatasi atau mengatur penggunaan cyberattack, cyberoperation, cybervandalism serta pencurian cyber yang dilakukan oleh atau terhadap aktor negara. Wilayah kebijakan ini terkait dengan pengembangan norma-norma cyber, atau upaya untuk menerjemahkan hukum internasional tentang konflik negara ke ranah online.

E. **Pemangku Kepentingan Cybersecurity dan Tantangan yang Dihadapi**



Ada banyak cara untuk memahami cybersecurity, dan demikian pula ada beragam pengampu yang dapat terlibat dalam pembuatan kebijakan cybersecurity. Meskipun tidak memungkinkan untuk menyebutkannya satu per satu, secara umum kita dapat mengidentifikasi lima kategori pengampu yang terlibat secara luas dalam pembuatan kebijakan cybersecurity, yaitu pemerintah (termasuk lembaga antar-pemerintah), komunitas teknis dan akademisi, sektor swasta / bisnis, dan organisasi masyarakat sipil (civil society organization / CSO). Setiap pemangku kepentingan di atas menghadapi berbagai tantangan dalam upayanya menghadapi cybersecurity. Tantangan-tantangan tersebut membentuk dan memandu tindakan mereka dalam proses pengambilan kebijakan di ranah cybersecurity.

1. Pemangku: **Pemerintah**

Meskipun seringkali dikatakan bahwa setiap organisasi pemerintah saat ini kerap berurusan dengan cybersecurity dalam berbagai bentuk, namun organisasi-organisasi utama yang bertanggung jawab atas cybersecurity antara lain adalah:

- Badan-badan standar teknis nasional yang ditugaskan membentuk dan menjaga standar teknis yang berlaku untuk keamanan informasi. Di Amerika Serikat, badan tersebut adalah US National Institute of Standards and Technology (NIST).
- Computer Emergency Response Teams (CERTs), yang juga dikenal sebagai tim siaga darurat komputer, serta Computer Security Incident Response Teams (CSIRTs). Para kelompok ahli ini, yang seringkali menjadi bagian dari lembaga penegak hukum atau intelijen, bertanggung jawab untuk merespon dan mencegah terjadinya insiden keamanan komputer, dan seringkali pula ditugaskan meningkatkan kesadaran publik.
- Kementerian Pertahanan, yang semakin menyadari prospek konflik cyber di masa depan dan cara menghadapinya.
- Kementerian Dalam Negeri atau Keamanan Nasional, yang umumnya bertanggung jawab mengawasi penegak hukum dan lembaga intelijen, mengkoordinasikan penyusunan strategi cybersecurity nasional, serta mengawasi cybersecurity infrastruktur penting.
- Kementerian Luar Negeri, yang mengkoordinasi kebijakan luar negeri dan melakukan negosiasi terkait kebijakan cybersecurity dan HAM.
- Kementerian Keuangan, yang mengelola anggaran untuk kebijakan cybersecurity.
- Lembaga penegak hukum, yang tidak hanya menangani cybercrime (seperti pencurian identitas, eksploitasi anak di ranah online, dan penjualan barang terlarang), namun juga kejahatan offline dengan unsur online, seperti kegiatan yang menggunakan pesan terenkripsi. Lembaga intelijen, yang umumnya bertanggung jawab dalam deteksi dan pencegahan insiden cybersecurity dan pemeliharaan infrastruktur penting. Di sejumlah negara, lembaga intelijen juga memiliki alat-alat pengawasan digital yang dapat memanfaatkan dan memanipulasi kelemahan sistem dan jaringan.

BOX 1 Tentang Pengampu dari Pemerintah Indonesia

Pendekatan lembaga pemerintah terhadap cybersecurity terutama berfokus pada ancaman nasional dan perlindungan infrastruktur nasional kritis. Sebagaimana disebutkan di atas, terdapat dua kementerian yang saat ini bertanggung jawab mengelola cybersecurity di Indonesia, yaitu Kementerian Koordinator Politik, Hukum dan Keamanan; serta Kementerian Komunikasi dan Informatika. Selain kedua kementerian tersebut, TNI, BIN, Kementerian Luar Negeri, dan baru-baru ini Lembaga Sandi Negara juga turut berkontribusi dalam diskusi seputar cybersecurity.

Kementerian Komunikasi dan Informatika (Kominfo) merespon kebutuhan akan suatu strategi keamanan internet dengan membentuk ID-SIRTII pada 2007. Tugas utama ID-SIRTII adalah melaksanakan pemantauan (monitoring), memelihara sistem deteksi dan peringatan dini terhadap ancaman di jaringan telekomunikasi, serta menangani tindakan hukum dalam sengketa cybersecurity. ID-SIRTII juga bertanggung jawab untuk menciptakan lingkungan yang aman untuk komunikasi berbasis internet di Indonesia, serta berfungsi sebagai pusat koordinasi isu-isu terkait cybersecurity. Pada 2010, Kominfo membentuk Direktorat Keamanan Informasi untuk membantu merumuskan dan melaksanakan kebijakan terkait cybersecurity, beserta norma, standar, prosedur dan kriteria di ranah keamanan informasi. Direktorat Keamanan Informasi diintegrasikan ke dalam struktur Kominfo, sementara ID-SIRTII bertindak sebagai lembaga negara independen.

Kementerian Koordinator Politik, Hukum dan Keamanan juga memiliki divisi cybersecurity-nya sendiri, yang bertujuan untuk menangani dan mengelola ancaman cybersecurity nasional. Jika Kominfo menjadi lembaga utama (lead) dalam hal cybersecurity sipil, maka Kemkopolhukam bertanggung jawab atas ancaman terkait keamanan nasional. Beberapa bulan lalu, divisi cyber menginisiasi sebuah Forum Cybersecurity, yaitu sebuah kelompok informal untuk mendiskusikan isu-isu yang terkait dengan serangan cyber dan tata kelola cyber. Kelompok informal ini terdiri dari aktor-aktor kejahatan cyber yang meliputi perwakilan bisnis hingga kepolisian dan organisasi masyarakat sipil.

Lembaga Sandi Negara (Lemsaneg) adalah aktor penting lainnya yang telah mulai terlibat dalam diskusi-diskusi seputar cybersecurity di Indonesia. Lemsaneg memiliki versi tata kelola cyber sendiri dan berpotensi memimpin koordinasi cybersecurity di Indonesia.

Terdapat perbedaan dalam pendekatan yang digunakan berbagai lembaga pemerintah. Lembaga-lembaga yang terkait erat dengan penegak hukum biasanya lebih berfokus pada isu-isu kejahatan cyber, sementara yang terkait dengan militer umumnya lebih berfokus pada spionase cyber dan terorisme cyber. Meskipun memiliki pendekatan serupa terhadap cybersecurity, aktor-aktor pemerintah ini masih memiliki mekanismenya masing-masing untuk menangani serangan cyber. Ketiadaan sebuah lembaga koordinator untuk hal ini merupakan salah satu alasan aktor-aktor ini bergerak secara tersekat.

Selain itu, Indonesia juga sudah memiliki Badan Siber dan Sandi Negara (BSSN) sejak 2017 lalu sebagai lembaga non teknis kementerian. Presiden Joko Widodo (Jokowi) telah menandatangani Peraturan Presiden (Perpres) No. 133 tahun 2017 tentang Perubahan atas Perpres No. 53 tahun 2017 tentang Badan Siber dan Sandi Negara pada 16 Desember 2017. BSSN diketuai oleh Mayjen (Purn) TNI Djoko Setiadi sebagai Kepala Badan Siber dan Sandi Negara (BSSN) di Istana Negara, pada 3 Januari 2018. Sebenarnya BSSN bukan lembaga baru, sebab merupakan revitalisasi Lembaga Sandi Negara (Lemsaneg) dengan tambahan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Kemkominfo).

Dengan pertimbangan bahwa bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional, pemerintah memandang perlu dibentuk badan dengan menata Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara, guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber.

Atas dasar pertimbangan tersebut, pada 19 Mei 2017, Presiden Jokowi telah menandatangani Peraturan Presiden (Perpres) Nomor: 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Sebagian pihak beranggapan BSSN dibentuk berkaitan dengan Tahun Politik Pilkada 2018 dan Pemilu 2019. Sesungguhnya ide pembentukan sebuah institusi gabungan siber dan Lemsaneg sudah lama. Sejak naskah akademisi Badan Siber yang dibuat oleh pokja Desk Keamanan Siber Nasional, Deputi VII, Kemenko Polhukam (2014) era Presiden Susilo Bambang Yudhoyono hingga Presiden Jokowi. Bahkan sejak era Orde Baru, Pemerintah mempunyai badan koordinasi bidang Telematika dibawah Presiden, dikenal dengan TKTI (Tim Koordinasi Telematika Indonesia) hingga era Reformasi Presiden Megawati.

Tugas BSSN adalah membangun ekosistem ranah siber Indonesia yang kuat dan aman. Selain itu BSSN juga menjadi penyelenggara dan pembina persandian negara dalam menjamin keamanan informasi, utamanya yang berklasifikasi milik pemerintah atau negara, dengan tujuan untuk menjaga keamanan nasional. BSSN berfungsi untuk mendeteksi, mencegah, dan menjaga keamanan siber mengingat banyak aksi-aksi kejahatan yang memanfaatkan dunia maya dalam beberapa waktu ke belakang.

Secara mendetail, fungsi BSSN antara lain:

- Identifikasi, deteksi, proteksi, dan penanggulangan e-Commerce
- Persandian
- Diplomasi siber
- Pusat manajemen krisis siber
- Pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber

Membasmi hoaks yang banyak beredar di dunia maya juga termasuk dalam fungsi BSSN. Lebih luas lagi, fungsi BSSN mencakup pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi. BSSN berperan dalam mengawal Indonesia memasuki era ekonomi digital (e-Commerce), big data, dan Fintech, yang selalu dibayangi serangan siber. Menkominfo Rudiantara menegaskan, untuk menjaga kesinambungan keamanan siber dan informasi nasional, maka ID-SIRTII tetap menjalankan tugasnya di Kominfo hingga siap dilaksanakan oleh BSSN, jika BSSN sudah memiliki anggaran dan struktur organisasinya.

Program Jangka Panjang BSSN adalah memberikan perlindungan kepada masyarakat Warga Negara Indonesia (WNI) di samping tugas mengamankan instansi pemerintah, BUMN, dan sektor swasta dengan batasan peraturan untuk dapat memenuhi harapan Presiden Jokowi. BSSN dirancang dengan model kolaborasi antara pemerintah, swasta, akademisi, beserta masyarakat, dengan doktrin pertahanan defensif, melakukan fungsi perlindungan, deteksi dini, prefentif (pencegahan), identifikasi, penanggulangan, dan recovery (restorasi/pemulihan).

Koordinasi fungsi keamanan siber cukup kompleks, melibatkan:

1. Kementrian Luar Negeri terkait kerjasama dan diplomasi siber bilateral, regional dan multilateral.
2. Kementrian Pertahanan dan TNI terkait Perang Asimetris dan Proxy diranah Siber.
3. Polri terkait Penanggulangan dan Penindakan Kejahatan Siber.
4. BIN terkait Human Intelijen.
5. Lemsaneg terkait Signal Intelijen dan Persandian menjadi BSSN.
6. Desk Siber dan ID-SIRTII proteksi siber yang ke depan akan dilebur ke BSSN.
7. Kominfo termasuk penampisan dan Pengaisan Siber, di mana direktorat
8. Keamanan Informasi dilebur ke BSSN.

Ketua BSSN, Djoko Setiadi, menekankan agar BSSN dapat melakukan koordinasi dan semua stakeholder keamanan siber selalu saling mengisi, melakukan back-up, serta menghindari duplikasi dan perbedaan dari unsur keamanan dan kemampuan siber yang ada di berbagai instansi dalam negeri, seperti penanganan kejahatan siber dan ancaman terorisme oleh Dittipidsiber (Direktorat Tindak Pidana Siber), Polri; Perang Siber dan Proxy War oleh institusi militer, Mabes TNI, Desk Siber di Kemenko Polhukam; spionase siber oleh Badan Intelijen Negara (BIN). Di tataran Global, US Department of Homeland Security; Divisi Keamanan Siber Nasional dan US Cyber Command meningkat dua kali lipat sejak dibentuk. NSA (National Security Agency), proyek DARPA seperti TOR (The Onion Router), Dark Webdan CINDER (Cyber Insider Threat), Departmen of Defence (DoD) di AS juga merekruit komunitas dan pakar hacker seperti Peiter Zatko, Mudge (2010) berhadapan dengan whistleblower, Julian Assange dan Edward Snowden.

Apakah BSSN akan meniru instansi NSA yang dapat melakukan penyadapan terhadap pembicaraan melalui saluran telekomunikasi global, bahkan menyadap media sosial dan pesan instan seperti WhatApp yang kini sangat populer di Indonesia? Menurut Djoko Setiadi, konten tidak ada batasnya demikian juga dengan ruang dan waktu di dunia siber. Statemen Menkominfo, Rudiantara, yang menyambut baik lahirnya BSSN, masih menekankan kewenangan terkait media sosial berada di Ditjen Aptika, Kominfo dengan mesin penampisan, robot crawling, dan pengais konten dengan kata kunci negatif, namun ke depan Kominfo tentu akan koordinasi dan sharing insight dengan BSSN.

Tantangan

Kesulitan dalam mendigitalkan layanan pemerintah untuk membuat layanan publik lebih efektif, dan di saat yang sama membangun kapasitas dan pengetahuan teknis lembaga pemerintah dan karyawan di sektor publik.

Tidak cukup tersedianya ahli teknologi dan ahli teknis keamanan untuk merancang dan melaksanakan strategi cybersecurity.

Risiko yang terjadi akibat sifat cybersecurity yang lintas-negara, yang membuat negara dengan strategi ketahanan cybersecurity yang lemah dapat mengganggu cybersecurity negara-negara lainnya.

Penggunaan alat anonimisasi, misalnya untuk memblokir chain currencies atau enkripsi, dalam kejahatan yang menggunakan internet, semakin mempersulit pembuatan kebijakan.

Selalu munculnya teknologi dan sistem baru dari waktu ke waktu memerlukan pemutakhiran sistem pengawasan dilakukan secara berkala.

Adanya penyedia layanan komunikasi jenis baru yang seringkali berdomisili di yurisdiksi negara lain serta memerlukan perlakuan berbeda dibandingkan dengan perusahaan telekomunikasi tradisional.

Bentuk cybercrime baru seperti ransomware, pencurian identitas, pendekatan seksual (grooming) dan pelecehan seksual melalui ranah siber.

Kebutuhan untuk menghadapi cyberattack dan bentuk konflik antarnegara lain akibat tidak adanya norma dan peraturan yang berlaku internasional yang mengatur perilaku negara.

2. Pemangku: **Komunitas Teknis dan Akademisi**

Di seluruh dunia, terdapat lebih dari 200 organisasi pengembangan standar (standards development organisations/SDO) yang mengembangkan standar teknis terkait cybersecurity. Beberapa di antaranya adalah:

- International Organisation for Standardisation (ISO), yaitu sebuah organisasi internasional tempat berkumpulnya berbagai badan standar teknis nasional.
- Internet Engineering Task Force (IETF), yaitu sebuah organisasi standar terbuka tanpa persyaratan keanggotaan formal yang mengembangkan dan mempromosikan standar internet sukarela, khususnya yang terdiri dari internet protocol suite (TCP/IP). Setiap orang dapat menjadi bagian dalam IETF dan setiap keputusan dibuat berdasarkan konsensus. Di dalam organisasi ini terdapat sebuah kelompok kerja yang dibentuk untuk mengurusi keamanan, serta terdapat pula sebuah kelompok peneliti yang meneliti implikasi HAM pada lapisan teknis.

- Internet Architecture Board (IAB), yaitu organisasi yang bertugas mengawasi IETF, dan merupakan komite yang bertugas mengawasi perkembangan teknis dan rekayasa di internet. Awalnya organisasi ini adalah badan pemerintah AS, namun menjadi independen pada 1992. Selain melakukan pengawasan terhadap protokol dan prosedur jaringan, IAB juga bekerja dengan Internet Corporation for Assigned Names and Numbers (ICANN).
- ICANN adalah sebuah organisasi nirlaba yang bertanggung jawab untuk mengkoordinasi pemeliharaan database identifier unik yang terkait dengan namespace internet. Tugas utama ICANN adalah mengelola Domain Name System (DNS), top-level domain, operasi root name server, serta memberikan internet protocol address space untuk IPv4 dan IPv6.

Indonesia memiliki beberapa CERT dan tim respon insiden keamanan kritis (Critical Security Incident Response Team/CSIRT) yang dibentuk dan diselenggarakan oleh pemerintah dan sektor swasta. Di antara tim-tim tersebut yang paling sering disebutkan adalah ID-CERT dan ID-SIRTII/CC karena peran dan sejarah mereka. ID-CERT (http://cert.id/) adalah tim tanggap darurat komputer pertama di Indonesia. ID-CERT didirikan pada 1998 oleh Budi Rahardjo dan merupakan sebuah tim berbasis komunitas untuk melakukan koordinasi teknis independen. Tim ini adalah salah satu pendiri Forum APCERT (Asia Pacific Computer Emergency Response Team). Sementara itu Tim Tanggap Insiden Keamanan Indonesia dari Pusat Koordinasi Infrastruktur Internet (The Indonesia Security Incident Response Team of the Internet Infrastructure Coordination Center/ID-SIRTII/CC) adalah tim tanggap insiden nasional Indonesia. Tim ini dibentuk pada 2003 oleh delapan pemangku kepentingan dari berbagai sektor, dan pusat ini berfungsi sebagai poin kontak bagi CERT domestik dan internasional. Pemangku kepentingan pertama ID-SIRTII/CC adalah Komkominfo, Polri, Kejaksaan Agung, Bank Indonesia, APJII, Asosiasi Warung Internet, Asosiasi Kartu Kredit Indonesia, dan Mastel. Lihat http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html, diakses pada 15 September 2016.

Sebagai anggota FIRST, APCERT dan OIC-CERT, ID-SIRTII/CC terlibat aktif dalam pelatihan, lokakarya maupun pertemuan regional, serta menjalankan program pelatihan dan lokakarya domestik yang kuat untuk pemerintah dan pekerja TIK sektor swasta (ASPI 2015).

Selain tim tanggap darurat komputer di atas, masih terdapat setidaknya 14 CERT/CSIRT lain di Indonesia yang dapat dilihat pada daftar berikut.

Daftar CERT/CSIRT di Indonesia

No.	CERT/CSIRT	Fungsi	Website
1.	ID-CERT	Publik	http://cert.id/
2.	ID-SIRTII/CC	Publik	http://idsirtii.or.id/
3.	Jabar-CSIRT	Berbasis daerah	
4.	JabarAcad-CSIRT	Berbasis daerah	
5.	JabarProv-CSIRT	Berbasis daerah	
6.	Jatim-CSIRT	Berbasis daerah	
7.	JogjaPG-CSIRT	Berbasis daerah	
8.	AcadCSIRT	Berbasis sektor	http://acad-csirt.or.id/
9.	ID.GovCSIRT	Berbasis sektor	http://govcsirt.kominfo.go.id/
10.	BPPT-CSIRT	Internal CSIRT	
11.	CSOC-Telkom	Internal CSIRT	
12.	IT Security Mandiri Team	Internal CSIRT	
13.	XL-CSIRT	Internal CSIRT	
14.	National Defense sector	CSIRT -	
15.	Pustekkom, Kementerian Pendidikan dan Kebudayaan	CSIRT - fungsi serupa	
16.	Direktorat Keamanan Perdagangan, Kementerian Perdagangan	CSIRT - fungsi serupa	

Sumber: ID-CERT (2016)

Tidak seperti ID-CERT dan ID-SIRTII/CC, CERT/CSIRT ini bersifat tertutup, yang beberapa di antaranya melayani kelompok atau komunitas terbatas dan terikat pada wilayah geografis tertentu.

Tantangan

Bagaimana memastikan adanya standar teknis yang sukarela disusun, disepakati, diadopsi dan dilaksanakan bersama.

Upaya terbuka maupun tertutup dari sejumlah negara untuk melanggar standar teknis yang telah ada ataupun tindakan yang bertujuan untuk mengendalikan proses pengembangan standar-standar teknis.

3. Pemangku: **Sektor Swasta / Bisnis**

Infrastruktur internet sebagian besar dimiliki dan dioperasikan oleh entitas swasta. Hal ini tentu saja membuat aktor ini memiliki kepentingan besar dalam cybersecurity, antara lain karena:

- Lembaga keuangan adalah salah satu pengembang dan promotor utama standar-standar teknis terkait cybersecurity.
- Produsen software dan hardware berkewajiban menjamin keamanan produk mereka di seluruh rantai pasok.
- Perusahaan teknologi dan penyedia layanan internet dan aplikasi seringkali dihadapkan pada tindakan negara yang mengatasnamakan cybersecurity, atau terjebak dalam konflik dengan pemerintah terkait pertanyaan seputar tanggung jawab dan liabilitas cybercrime. Sektor swasta semakin diakui luas sebagai pengampu kunci dalam inisiatif dan ruang kebijakan cybersecurity.
- Para vendor antivirus dan cybersecurity serta penyedia layanan amat penting untuk membantu aktor publik dan swasta dalam mencegah dan merespon ancaman siber. Mereka merupakan sumber penelitian dan data tentang cybersecurity, misalnya terkait kekerapan dan jenis pelanggaran cybersecurity.

BOX 2 Tentang Pengampu dari Sektor Swasta Indonesia

Dalam hal pengembangan teknologi, sektor swasta hampir selalu lebih maju dibandingkan pemerintah dan masyarakat sipil. Hal ini berlaku pula pada tata kelola cybersecurity. Di Indonesia, sektor bisnis seringkali tampak lebih aktif dalam diskusi tentang kebijakan cyber dan pengelolaan cyber.

Pendekatan sektor bisnis terhadap cybersecurity tampak cukup jelas. Sektor bisnis berkepentingan khususnya untuk melindungi infrastruktur dan perkembangan bisnis. Karena itu tidak mengejutkan ketika sektor bisnis membentuk sebuah CSIRT/CERT yang maju dan amat mapan untuk cybersecurity. Dalam hal regulasi, sektor swasta mayoritas menggunakan UU ITE dan UU Telekomunikasi sebagai basis untuk mengembangkan alat (tool) untuk mencegah serangan cyber. Namun, perlu dicatat bahwa saat ini terdapat kebutuhan mendesak untuk memiliki peraturan yang dapat melindungi kepentingan sektor bisnis, seperti peraturan OTT dan peraturan privasi data, yang keduanya masih berada pada tahap awal proses penyusunan.

Sektor swasta memiliki pengetahuan yang baik mengenai cybersecurity karena sektor ini memiliki sumber daya untuk mengembangkan tool dan sistem yang diperlukan untuk perlindungan cyber. Namun, pengamatan kami menunjukkan bahwa meskipun mereka memiliki pengetahuan dan sumber daya, mereka belum menganggap membantu pemerintah untuk mengembangkan mekanisme cybesecurity yang baik sebagai prioritas utama. Keterlibatan sektor swasta dalam diskusi kebijakan karenanya bukan berarti mereka akan berpartisipasi dalam meningkatkan kapasitas dan kapabilitas pemerintah dalam mengelola cybersecurity. Meskipun pembangunan kapasitas dan kapabilitas bukan menjadi tanggung jawab utama sektor swasta, mereka memiliki sumber daya yang mendukung, sehingga jika mereka dapat berpartisipasi, akan sangat membantu tata kelola cybersecurity di Indonesia.

Tantangan

- Kesulitan untuk beroperasi lintas yurisdiksi, yang berarti dihadapkan pada hukum, penalti maupun rezim regulasi yang berbeda-beda.
- Berpotensi terkena pencemaran nama baik serius serta gugatan perdata jika terlibat atau bertanggung jawab atas suatu insiden cybersecurity.
- Tekanan untuk membantu pemerintah dalam menegakkan cybersecurity serta melawan cybercrime dan terorisme, yang dapat mencakup pembuatan kebijakan dan pelaporan konten, mematikan jaringan, pemblokiran layanan, bahkan mengkompromikan keamanan produk mereka sendiri untuk membantu pengawasan oleh pemerintah.
- Keharusan membangun kapasitas internal untuk menjaga keamanan informasi dan jaringan.
- Insentif untuk menjaga kerahasiaan data yang dapat menimbulkan risiko dan serangan siber dengan mengatasnamakan privasi data dan potensi pencemaran nama baik

4. Pemangku: **Organisasi Masyarakat Sipil / CSO**

Masyarakat sipil adalah pemain yang tingkat keaktifannya paling rendah dalam ranah kebijakan cybersecurity. Meskipun terdapat banyak kerja penting dan signifikan yang dilakukan oleh pejuang HAM di berbagai wilayah kebijakan cybersecurity, masih terdapat banyak wilayah kebijakan cybersecurity di mana masyarakat sipil tidak dilibatkan secara substansial. Faktor-faktor yang menyebabkan hal ini antara lain adalah:

- Kurangnya pendanaan dan kapasitas untuk mengikuti diskusi kebijakan cybersecurity
- Sifat tertutup dari kebanyakan forum kebijakan cybersecurity
- Kurangnya pemahaman teknis

Masyarakat sipil sejatinya telah terlibat dalam sejumlah isu kebijakan yang beririsan luas dengan area cybersecurity dalam dialog tata kelola internet. Hal tersebut semisal pada isu privasi dan pengintaian (surveillance) yang dekat sekali dengan dinamika kebebasan berekspresi. Masyarakat sipil juga telah lama berperan dan terlibat aktif dalam isu-isu seperti perlindungan anak di ranah online, yang notabene terkait erat dengan cybercrime.

BOX 3 Tentang Pengampu dari Organisasi Masyarakat Sipil Indonesia

Dalam diskusi-diskusi seputar cybersecurity, masyarakat sipil tampak tertinggal, khususnya dalam isu privasi dan perlindungan data pribadi. Pengamatan kami menunjukkan bahwa hanya beberapa komunitas yang secara aktif terlibat dalam isu cybersecurity, yang sebagian besarnya menggunakan pendekatan HAM.

Masyarakat sipil (dan akademisi) dapat berkontribusi kepada cybersecurity dengan meningkatkan kesadaran keamanan serta membangun budaya keamanan, sehingga dapat menutup keterbatasan sektor publik dan swasta (DAKA, 2013). Sejalan dengan visi ini, beberapa aktor sudah mulai bekerja untuk mengisi kesenjangan ini. Kasus-kasus terkait perlindungan anak online, misalnya, menunjukkan bagaimana akademisi dan masyarakat sipil dapat berkontribusi terhadap tata kelola cybesecurity.

Karena Indonesia tidak memiliki lembaga resmi yang diakui untuk memberikan dukungan kelembagaan terkait perlindungan online anak, aktor-aktor ini memberikan jalan untuk menangani insiden terkait perlindungan online anak. Salah satu aktor tersebut adalah ICT Watch dengan program “Internet Sehat”-nya, yang memenangkan penghargaan WSIS Champion Award 2016 dan WSIS Winner Award 2017 dari PBB.. Melalui program tersebut, ICT Watch berupaya untuk menunjukkan bahwa masyarakat dapat bertanggung jawab dalam menjalankan kegiatan online mereka, dari menyusun modul untuk orang tua dan guru, hingga menerbitkan buku komik untuk anak/remaja tentang keselamatan internet serta mendorong masyarakat untuk berpartisipasi dalam berbagai kegiatan online dan offline.

Terkait pemerintah, organisasi masyarakat sipil seringkali mendekati cybersecurity dari berbagai perspektif. Misalnya, organisasi HAM seperti Elsam menggunakan pendekatan kebebasan berekspresi, sementara ICT Watch menggunakan pendekatan yang lebih berbasis teknologi. CSIS adalah salah satu aktor masyarakat sipil baru yang menggunakan pendekatan ekonomi digital dan keamanan nasional. Prinsip-prinsip dasar berbeda yang digunakan ini kemudian menghasilkan prioritas yang berbeda pada setiap aktor yang saling melengkapi satu sama lain.

Tantangan

- Semakin maraknya kegiatan berbagai pihak yang mengusung bendera cybersecurity, tanpa adanya kejelasan tentang apa dan mengapa hal tersebut sebenarnya harus dilakukan.
- Kebingungan dalam memahami hukum dan kebijakan terkait internet, kurangnya transparansi di para pengampu yang melakukan pemantauan dan/atau mengendalikan penggunaan internet.
- Kurangnya transparansi dalam penggunaan kemampuan cyberattack oleh suatu negara.
- Perubahan yang cepat dalam ranah teknologi, kurangnya pemahaman publik dan literasi digital (termasuk kurangnya penggunaan dan pemahaman alat perlindungan privasi online di kalangan masyarakat umum), serta kesulitan dalam menyediakan akses sumber daya terkait isu teknis untuk khalayak umum.

Ringkasan

Dari pemetaan aktor-aktor cybersecurity ini, kami menemukan dua 'sayap' berbeda, yaitu yang bersandar pada perspektif HAM, serta yang sangat dipengaruhi perspektif pertahanan. Secara umum, sayap kedua lebih menggunakan argumen yang kaku dalam debat, yang sebagian di antaranya didasarkan pada premis yang salah. Penelitian ini juga mengamati bahwa mereka yang memegang perspektif pertahanan cenderung lebih penuh kewaspadaan dibandingkan dengan yang berpegang pada perspektif HAM.

Terkait tata kelola cybersecurity nasional, masing-masing aktor utama di atas tampak memahami bahwa ada kebutuhan untuk memiliki sebuah lembaga koordinasi untuk mengelola berbagai pemahaman berbeda tentang cybersecurity. Namun, saat ini terjadi debat yang semakin panas di tengah kompleksitas isu ini. Masih perlu diamati apakah Indonesia akan mendorong salah satu unit struktur keamanannya untuk mengelola cybersecurity di seluruh lembaga pemerintahan, atau mengembangkan sebuah badan koordinasi untuk membantu berbagai lembaga mengelola jaringan mereka secara otonom dengan kemungkinan berkoordinasi jika diperlukan.

F. Hak Asasi Manusia (HAM) dan Cybersecurity

Seringkali dikatakan bahwa cybersecurity terkait erat dengan perlindungan informasi dan jaringan. Keduanya adalah penting dalam perspektif HAM. Namun mengapa?

Informasi amat vital untuk kelancaran hidup kita sehari-hari. Setiap orang membuat dan membagikan berbagai data pribadi setiap harinya, dari email dan data kesehatan hingga rincian akun bank serta catatan pengalaman kerja. Data ini, terlebih jika dikumpulkan, dapat mengungkapkan data paling sensitif seseorang, seperti orientasi seksual, kegiatan politik maupun lokasi geografis.

Data ini umumnya disimpan, dimiliki dan dikelola oleh entitas swasta atau pemerintah. Dari sudut pandang HAM, hal ini menciptakan implikasi serius. Tanpa adanya upaya cybersecurity yang kuat, informasi tersebut tidak hanya dapat diakses dan dicuri, tapi juga dihapus, diubah dan dimodifikasi.

Salah satu contoh kasus ini adalah yang terjadi pada US Office of Personal Management pada 2015. Kantor tersebut diretas dan menyebabkan terbukanya data pribadi sensitif dari 22 juta orang, termasuk catatan riwayat kesehatan mental serta data penyalahgunaan obat-obatan dan alkohol yang pernah dilakukan. Serangan seperti ini berdampak langsung terhadap HAM, termasuk hak atas privasi, yang dapat secara langsung mengancam kehidupan orang yang bersangkutan bahkan di ranah offline (dunia nyata).

Namun alih-alih mengevaluasi lemahnya sistem penjagaan penyimpanan data, pemerintah saat itu menyatakan peretasan tersebut tidak lebih dari sekadar insiden diplomatik, dan menjanjikan akan melakukan tindakan pembalasan terhadap pemerintah negara asing yang dianggap bertanggung jawab atas peretasan tersebut.

Selain data pribadi yang dipegang oleh entitas swasta atau pemerintah, terdapat pula data pemerintah dan perusahaan. Data pemerintah juga termasuk data sensitif, meskipun tidak terkait dengan orang per orang tertentu sebagaimana data pribadi. Data pemerintah dapat berisi informasi negosiasi dagang, intelijen asing, lokasi pasukan, rahasia militer maupun proses pengadilan. Sementara itu data perusahaan dapat berisi informasi tentang kesepakatan, aset, paten, hingga rahasia dagang.

RANSOMWARE WANNACRY, SERANGAN GLOBAL YANG MENGINFEKSI RATUSAN RIBU KOMPUTER

Serangan ransomware WannaCry terjadi pada Mei 2017 di seantero dunia oleh WannaCry ransomwarecryptoworm. Target utamanya adalah semua komputer yang menjalankan sistem operasi Microsoft Windows dengan melakukan enkripsi data dan menuntut pembayaran dalam bentuk Bitcoin. Serangan tersebut disebarkan melalui EternalBlue, sebuah celah pada sistem Windows yang lebih tua yang dirilis oleh The Shadow Brokers beberapa bulan sebelum serangan tersebut.

Sementara Microsoft telah merilis patch sebelumnya untuk menutup eksploitasi, sebagian besar penyebaran WannaCry berasal dari organisasi yang belum menerapkannya, atau menggunakan sistem Windows lama. WannaCry juga memanfaatkan instalasi backdoor ke sistem yang terinfeksi. Serangan tersebut dihentikan dalam beberapa hari setelah ditemukannya patch darurat yang dikeluarkan oleh Microsoft, dan ditemukannya sebuah saklar pembunuh yang mencegah komputer yang terinfeksi menyebarkan WannaCry lebih jauh lagi. Serangan tersebut diperkirakan telah mempengaruhi lebih dari 300.000 komputer di 150 negara, dengan total kerugian berkisar antara ratusan juta sampai miliaran dolar. Pakar keamanan percaya dari evaluasi awal cacing bahwa serangan tersebut berasal dari Korea Utara atau agensi yang bekerja untuk negara tersebut. Pada bulan Desember 2017, Amerika Serikat, Inggris dan Australia secara resmi menegaskan bahwa Korea Utara berada di balik serangan tersebut.***

JARINGAN

Jaringan adalah suatu infrastruktur yang memindahkan dan menyimpan informasi serta memfasilitasi keterhubungan dari berbagai alat.

Dari sudut pandang HAM, jaringan adalah penting karena kelancaran berbagai layanan publik dan swasta utama bergantung pada keamanan jaringan. Layanan yang dimaksud mencakup telepon seluler, pembayaran elektronik, sistem perbankan, jaringan transportasi kota, layanan gas dan listrik, hingga lampu lalu lintas. Upaya perusakan jaringan dapat mengakibatkan dampak langsung dan cepat terhadap kehidupan banyak orang, khususnya dengan semakin banyaknya objek dan orang yang terkoneksi dengan internet saat ini.

Berdasarkan sudut pandang inilah, berbagai upaya dirancang untuk mengamankan informasi dan jaringan yang dapat dipandang sebagai prasyarat untuk tegaknya HAM, antara lain:

- Hak atas privasi dan perlindungan informasi personal
- Hak atas kebebasan berekspresi dan akses kepada informasi
- Hak atas kebebasan berkumpul dan berserikat
- Hak atas kebebasan dan keamanan pribadi
- Hak anak untuk bebas dari eksploitasi dan kekerasan/pelecehan

MATI LAMPU DI UKRAINA

Pada Desember 2015, perusahaan listrik Ukraina Prykarpattyaoblenergo melaporkan terjadinya mati listrik di ibu kota provinsi Ivano-Frankivsk. Dua instalasi lainnya juga mengalami mati listrik di saat yang sama, namun tidak melaporkannya. Belakangan diketahui bahwa peristiwa di ketiga instalasi tersebut disebabkan oleh satu Malware, yaitu BlackEnergy, yang menunjukkan bahwa hal itu dilakukan secara sengaja sebagai suatu serangan cyber. Analisis terhadap Malware tersebut mengungkapkan bahwa Malware tersebut dirancang untuk menghapus memori sistem. Akhirnya, pemerintah Ukraina menuduh Rusia sebagai pihak yang bertanggung jawab atas serangan tersebut.

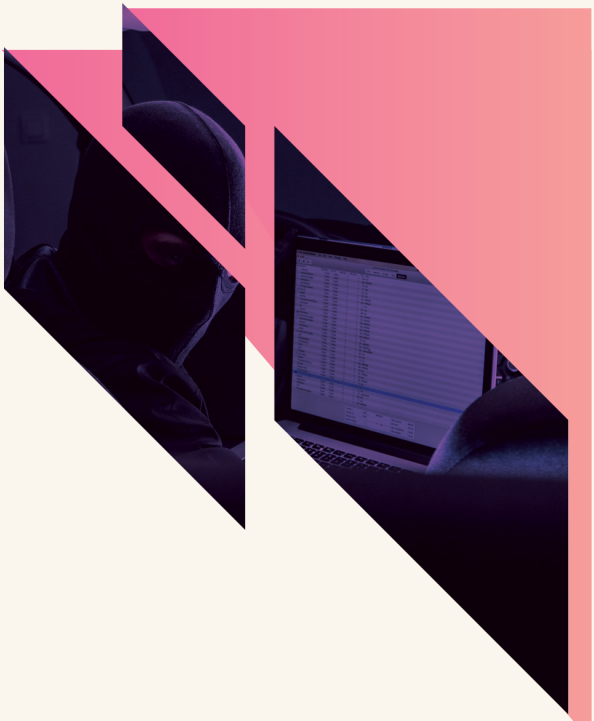
Bagaimanapun, pembuatan kebijakan cybersecurity juga dapat berimplikasi negatif dan serius terhadap penegakan HAM. Sebagaimana telah ditunjukkan di atas, berbagai kebijakan telah diambil yang bertujuan untuk mencegah, mendeteksi atau menginvestigasi ancaman dan kejahatan di ranah online. Namun, upaya-upaya tersebut juga dapat bersinggungan dengan HAM secara perorangan. Beberapa contoh di antaranya adalah:

- Upaya untuk mencegah anonimitas atau kerahasiaan di ranah online, termasuk larangan layanan enkripsi. Hal ini seringkali dijelaskan sebagai cara untuk memerangi cybercrime, namun sebenarnya juga dapat menghambat kebebasan berekspresi serta menghalangi seseorang untuk menikmati hak privasinya. Tanpa akses kepada layanan yang terenkripsi, para pejuang HAM, jurnalis, minoritas dan kelompok oposisi tidak dapat lagi berkumpul dengan bebas tanpa merasa takut akan terdeteksi.
- Hukuman serta pembatasan terhadap kelompok 'hacktivist' atas nama cybersecurity yang seringkali tidak proporsional dan menghambat kebebasan berekspresi, komunikasi dan kebebasan berkumpul.
- Pelaksanaan sistem pengintaian masal (mass surveillance), yang melanggar esensi hak privasi dan menciptakan masyarakat surveillance yang tercerabut dari kemampuan berpikir progresif, inovatif dan kreatif.

- Pemblokiran konten dan/atau penerapan filter internet secara serampangan karena tanpa merujuk pada prosedur yang transparan dan akuntabel, sehingga menghambat kebebasan berekspresi di internet serta meningkatkan jumlah penyensoran membabi-buta atas nama penanganan kejahatan siber.
- Manipulasi infrastruktur, mematikan sambungan internet, serta pelambatan internet (throttling) selama terjadinya politik, pemilu dan demonstrasi, yang mengancam hak berekspresi dan menyampaikan pendapat oleh seseorang.
- Dikumpulkannya berbagai kelemahan untuk dimanfaatkan dalam operasi siber ofensif, yang pada akhirnya melanggar tujuan cybersecurity itu sendiri karena menyebabkan informasi dan jaringan tidak aman dan lebih rentan terhadap serangan.

Pemaknaan cybersecurity yang timpang dapat menyebabkan terjadinya sekuritisasi skala besar di internet. Internet lantas dipandang sebagai medan laga, sebuah ranah yang dikuasai para penjahat, pelaku tindak kriminal dan teroris, bukan lagi sebuah ranah untuk pendidikan, komunikasi, emansipasi dan berdemokrasi sebagaimana yang seharusnya.

Dampak merugikan dari implementasi kebijakan cybersecurity terhadap HAM tidak selalu akibat kesengajaan. Namun hal ini selalu dapat diprediksi dan dihindari, jika kita semua bersedia menginvestasikan waktu, sumber daya dan kemauan untuk duduk bersama merumuskannya. Maka jelaslah bahwa pendekatan multistakeholder menjadi penting dan signifikan dalam penyusunan kebijakan terkait cybersecurity.



Jika Anda melakukan pencarian kata ‘sekuritisasi’ di mesin pencari, Anda akan disajikan berbagai definisi, yang kebanyakan terkait keuangan. Dalam ranah kebijakan cybersecurity, istilah ini memiliki makna spesifik dan berbeda, yang berasal dari mazhab pemikiran dalam teori hubungan internasional yang bernama Copenhagen School (Mazhab Copenhagen), yang pendukungnya menyebut diri mereka sebagai ‘konstruktivis’, yang tertarik dalam memahami bagaimana suatu situasi dapat terjadi dan mengapa, atau bagaimana kita bisa memandang ‘realitas’ sebagai sebuah konstruksi sosial.

Menurut para ahli teori Copenhagen School, sekuritisasi adalah sebuah proses di mana sejumlah aktor (yang disebut sebagai aktor sekuritisasi) mengubah suatu isu menjadi isu keamanan. Isu tersebut, begitu dimaknai dengan cara ini, akan menarik perhatian dan sumber daya yang jauh lebih besar daripada ancaman itu sendiri, dan akhirnya menjustifikasi upaya keamanan berlebihan, seperti diumumkannya kondisi darurat atau dimatikannya internet. Teori ini sering digunakan untuk menjelaskan mengapa sejumlah ancaman bagi jiwa manusia seperti terorisme lebih mendapatkan perhatian dibandingkan isu lainnya di media dan pembuatan kebijakan.

Copenhagen School mengidentifikasi ciri-ciri utama ancaman yang telah mengalami sekuritisasi, yaitu:

- Ancaman tersebut tidak hanya dimaknai atau disajikan sebagai sesuatu yang berbahaya, namun juga bersifat mendesak, dekat dan eksistensial (artinya dapat mengancam keberadaan atau keselamatan/survival manusia)
- Ancaman tersebut disajikan sebagai ancaman bagi kedaulatan dan otonomi politik nasional
- Pesan ditekankan pada perlindungan keselamatan dan nilai kolektif dengan mengabaikan perlindungan pribadi

Terdapat banyak ‘aktor sekuritisasi’ potensial yang dapat dilibatkan dalam proses ini, yang dapat mencakup pejabat pemerintah, pengambil kebijakan lain, figur korporat, pelobi, hingga media.

Pada Juni 2012, United Nations Human Rights Council (UNHRC) mendeklarasikan dalam sebuah resolusinya bahwa "seluruh HAM yang dinikmati seseorang di ranah offline juga harus dilindungi di ranah online". Namun, sejak momen bersejarah ini, PBB maupun berbagai organnya serta berbagai mekanisme HAM regional lainnya terlihat masih lamban dalam memberikan panduan tentang apa yang harus dilakukan oleh negara untuk menegakkan perlindungan tersebut.

Hal ini masih menjadi wilayah yang masih berkembang dalam hukum HAM, dan sejauh ini hanya terdapat sedikit jawaban definitif tentang apa yang harus dan tidak boleh dilakukan oleh pemerintah maupun aktor swasta terkait cyberspace. Akan tetapi, sejumlah instrumen dan keputusan kunci memberikan sejumlah panduan dalam isu ini. Instrumen dan keputusan tersebut mewajibkan setiap tindakan, termasuk yang dilakukan atas nama cybersecurity, yang mengakibatkan pembatasan HAM di era digital, untuk memenuhi standar-standar berikut:

a. Tindakan tersebut harus diputuskan berdasarkan hukum.
   Tindakan melarang suatu kegiatan di internet atau penggunaan suatu layanan tertentu di internet tidak boleh lagi hanya didasarkan pada kebijakan atau perjanijan den gan penyedia layanan. Sekarang, tindakan tersebut harus didukung oleh legislasi yang akurat, publik dan transparan. Selain itu, pelaksanaannya harus diawasi oleh suatu badan peradilan atau independen. Dalam hal pengawasan (surveillance) rahasia, karena tingginya risiko terjadinya tindak kesewenang-wenangan dalam penerapannya, diperlukan suatu pengesahan resmi dari suatu lembaga hukum.

b. Tindakan tersebut harus dipandang diperlukan dalam suatu masyarakat demokratis
   Diperlukan artinya lebih dari sekadar 'berguna' atau 'dikehendaki'. Contohnya, meskipun pelarangan penggunaan end-to-end encryption mungkin dapat berguna, bukan berarti hal itu perlu untuk menegakkan cybersecurity. Dalam hal pengawasan rahasia, 'kebutuhan' dilakukannya tindakan pengawasan tersebut harus dapat dibuktikan secara nyata, antara lain misalnya tindakan tersebut memang diperlukan untuk menjaga lembaga demokrasi atau diperlukan untuk suatu operasi tertentu.

c. Tindakan tersebut harus proporsional dengan tujuan yang ingin dicapai

Ancaman yang disebabkan suatu pembatasan tidak boleh melebihi manfaat yang didapat. Ketika memperhitungkan ancaman yang ditimbulkan dari pembatasan terhadap internet, penting sekali untuk kembali mengingat peran inti dari hak kebebasan berekspresi, berserikat dan berkumpul dalam menjamin berjalannya dan akuntabelnya suatu demokrasi, serta bahwa pembatasan yang diterapkan terhadap internet tersebut dapat berdampak amat luas dan mempengaruhi semua orang di seluruh dunia. Ketika suatu pembatasan berdampak luas kepada seseorang yang tidak mengancam cybersecurity, negara harus memberikan justifikasi yang amat kuat untuk dapat melakukan pembatasan tersebut.

Jika ada tindakan lain yang dengan dampak yang minimal dapat mencapai tujuan yang sama, maka tindakan tersebutlah yang harus dipilih, sembari tetap memberikan justifikasi berbasis bukti kepada publik untuk pembatasan yang akan dilakukan. Tindakan yang bersifat tebang pilih lebih baik dibandingkan yang bersifat menyamaratakan, dan suatu analisis mengenai proporsionalitas harus memperhitungkan kemungkinan bahwa pelanggaran enkripsi dan anonimitas juga dapat dimanfaatkan oleh jaringan penjahat dan teroris yang menjadi sasaran tindakan tersebut.

"SELURUH HAM YANG DINIKMATI SESEORANG DI RANAH OFFLINE JUGA HARUS DILINDUNGI DI RANAH ONLINE" – UNHCR

BAB II

Cybersecurity Sebagai Keamanan Informasi

Keamanan informasi adalah tentang bagaimana menjamin bahwa data yang diciptakan, dikumpulkan, dihasilkan, diproses atau disimpan oleh suatu lembaga pemerintah, bisnis ataupun masyarakat terlindungi dari akses tanpa izin, gangguan, pencurian dan eksploitasi.

Dalam pengertian ini, cybersecurity juga tentang bagaimana mengambil langkah-langkah untuk membuat infrastruktur dan jaringan informasi menjadi lebih aman. Bagaimana caranya? Hal itu tentu saja tergantung pada apa/siapa Anda dan tindakan apa (teknis, hukum, atau tata kelola) yang dapat Anda lakukan untuk mengamankannya.

Setiap lembaga pemerintah, bisnis maupun masyarakat akan menghadapi berbagai risiko yang bentuknya beragam, berdasarkan pada informasi apa yang mereka pegang dan proses, serta untuk tujuan apa dan dengan cara bagaimana. Misalnya, risiko cybersecurity tertinggi bagi manajemen investasi keuangan bisa jadi adalah pada rentannya pencurian informasi rahasia ataupun manipulasi pada pasar investasi, bukan tentang bocornya data pribadi karyawan misalnya. Namun bagi institusi militer, menjaga data pribadi “karyawan”-nya adalah vital, terkait keamanan negara misalnya. Adapun bagi entitas layanan publik seperti rumah sakit, data pribadi pasien terkait riwayat kesehatan bukan tak mungkin adalah hal yang sakral dengan bobot risiko cybersecurity tertinggi ketimbang data karyawannya.

Pada intinya, baik pemerintah maupun perusahaan di seluruh dunia memiliki satu pandangan yang sama bahwa cybersecurity, dalam hal ini keamanan informasi, adalah prioritas kebijakan yang jelas dan mendesak. Akan tetapi, hal tersebut masih banyak diperdebatkan tentang bagaimana cara terbaik untuk menyusun kebijakan dan proses mencapai tujuan tersebut.

A. **Standar-Standar Teknis Internasional**

Terdapat lebih dari 1000 publikasi yang berupaya menetapkan standar-standar teknis tentang cybersecurity, namun belum ada satu pun yang secara komprehensif membahasnya. Hal ini menyebabkan terjadinya ketimpangan dan perpecahan dalam perkembangan standar teknis. Sebuah laporan US National Institute of Standards and Technology (NIST) pada Desember 2015, yang mengidentifikasi sepuluh area inti standarisasi cybersecurity (termasuk misalnya teknik kriptografi) menyatakan bahwa dari seluruh aplikasi kunci yang ada seperti cloud computing, manajemen darurat atau manajemen pemungutan suara, standar yang ada masih bersifat parsial, sama sekali tidak ada atau masih dikembangkan di berbagai area. Standar-standar teknis tersedia hanya pada sejumlah area standarisasi, seperti keamanan jaringan untuk aplikasi pemungutan suara.

ISO STANDARD 9564 – MANAJEMEN NOMOR IDENTIFIKASI PERSONAL (PIN)

Salah satu contoh dari sebuah standar teknis adalah ISO 9564, yang terkait dengan manajemen PIN dan keamanan bank ritel. Keamanan dalam suatu sistem perbankan modern amat bergantung pada interoperabilitas antarbank, retailer dan penerbit kartu, yang memerlukan adanya seperangkat peraturan dan praktik bersama tentang bagaimana suatu PIN boleh didapatkan, diotentikasi dan dipindahkan. Standar ISO memberikan peraturan dan praktik tersebut, yang mencakup panjang pin, spesifikasi alat entry PIN, hingga penerbitan dan enkripsi PIN.

Pengembangan standar secara tradisional didorong oleh pasar, dan selama ini lebih bersifat reaktif alih-alih antisipatif. Standar-standar dikembangkan oleh Standard Development Organisatons (SDO) di seluruh dunia, khususnya organisasi sukarela yang terdiri dari perorangan, ahli dan perwakilan perusahaan, yang bekerja berdasarkan konsensus. Dengan cara ini, pengembangan standar berjalan dari bawah ke atas (bottom-up) alih-alih atas ke bawah (top-down). Namun di sejumlah negara, badan-badan standar nasional amat dipengaruhi oleh pemerintah. Terdapat sejumlah perbedaan dalam pendekatan yang digunakan di Amerika Serikat, yang amat bergantung pada sektor swasta untuk mendorong pengembangan standar, serta Uni Eropa, yang menggunakan pendekatan top-down (misalnya melalui European Telecommunications Standards Institute).

Terdapat lebih dari 1000 publikasi yang berupaya menetapkan standar-standar teknis tentang cybersecurity, namun belum ada satu pun yang secara komprehensif membahasnya.

Saat ini masih ada sedikit ketidaksepakatan tentang peran inti yang dijalankan SDO dalam pengembangan standar-standar untuk cybersecurity, dan juga tentang apa tujuan pengembangan standar tersebut. Namun, proses negosiasi pengembangan standar untuk cybersecurity dapat berjalan lamban, bahkan tidak transparan dan tertutup bagi pihak luar. Lingkungan standar ini, menurut NIST, semakin hari menjadi semakin terpolitisasi, karena semakin banyak negara yang mulai melakukan 'forum shop' untuk mendukung kepentingan kebijakan publik tertentu dengan menghubungi berbagai SDO, dan memandang proses pengembangan standar sebagai peluang baik untuk mendorong diadopsinya sejumlah kebijakan yang mendukung agenda tertentu.

Selain akibat ketiadaan standar yang koheren, entitas sektor swasta juga sering mengeluhkan apa yang mereka anggap sebagai kurangnya informasi dan panduan terkait pelaksanaan standar, serta kurangnya kejelasan tentang apa standar yang harus mereka patuhi yang sesuai dengan kondisi demografis dan kebutuhan organisasi mereka. Selain itu, mereka juga mengalami kesulitan untuk mengetahui standar atau panduan apa yang harus dirujuk untuk menerapkan 'praktik terbaik'. Perusahaan swasta juga kewalahan dengan banyaknya standar di sejumlah area, sementara amat kekurangan standar di area yang lain, seperti standar terkait apa yang harus dilakukan karyawan dan kontraktor untuk melindungi cybersecurity.

Sebenarnya memang terdapat penekanan berlebihan terhadap standar-standar teknis, sementara standar terkait proses cenderung sedikit diabaikan (lihat halaman 15). Sebuah studi yang dilakukan oleh pemerintah Inggris pada 2015 mengungkapkan bahwa terdapat lebih dari 1000 publikasi tentang cybersecurity di seluruh dunia, yang 67 persen di antaranya berfokus pada standar-standar cybersecurity organisasi, dan hanya 3 persen yang terkait cybersecurity dan keamanan perorangan.

BOX 4 Global Conference on CyberSpace (GCCS)

Konferensi Global Dunia Maya atau yang dikenal dengan nama Global Conference on CyberSpace (GCCS) adalah salah satu forum global yang paling penting di mana dalam forum ini para pemimpin, pembuat kebijakan, pakar industri, lembaga penelitian dan advokasi, cyber wizard, dan sebagainya, berkumpul untuk membahas berbagai masalah dan tantangan dalam menggunakan ruang siber secara optimal. GCCS diadakan dengan tujuan untuk menetapkan "peraturan jalan" (rules of the road), terkait perilaku di dunia maya yang disepakati secara internasional, serta menciptakan dialog yang lebih fokus dan inklusif antara semua pihak yang memiliki kepentingan di internet (pemerintah, masyarakat sipil, dan industri) tentang bagaimana mengimplementasikannya.

GCCS pertama diselenggarakan di London, Inggris, pada 2011. Pada konferensi tersebut, sebanyak 700 delegasi secara global ikut berpartisipasi dan membantu dalam menetapkan peraturan dan pedoman untuk konferensi berikutnya. Konferensi kedua diadakan pada 2012 di Budapest, Hongaria, dengan fokus pada hubungan antara hak-hak di internet dan keamanan internet, yang dihadiri oleh 700 delegasi dari hampir 60 negara.

GCCS ketiga diadakan pada 2013 di Seoul, Korea Selatan, yang berfokus pada tema Open and Secure Cyberspace dengan jumlah partisipasi sebanyak 1.600 delegasi. Konferensi keempat (GCCS 2015) diadakan di Den Haag, Belanda. Hampir 1.800 anggota dari sekitar 100 negara berpartisipasi dalam konferensi ini, dan lebih dari 60 negara berpartisipasi dengan delegasi yang dipimpin tingkat Menteri.

Skala dan pentingnya GCCS berkembang secara signifikan di setiap konferensi. Sebuah mekanisme kelembagaan, GFCE (Global Forum on Cyber Expertise), pun dibentuk untuk meningkatkan Capacity Building. Adapun GCCS ke-5 dilaksanakan pada 2017 lalu di New Delhi, India, yang mengambil tema "Cyber4All: A Secure and Inclusive Cyberspace for Sustainable Development".

Sebelum pelaksanaan GCCS ke-5 tersebut, beberapa organisasi masyarakat sipil (Civil Society Organization/CSO) dari berbagai negara mengadakan workshop untuk mendorong tercapainya visi dunia maya yang menghargai hak-hak, didukung oleh proses pembuatan kebijakan yang terbuka, inklusif dan transparan. Hasil workshop tersebut disusun dalam sebuah pesan sebagai berikut:

Kepada para penyelenggara dan delegasi Global Conference on Cyberspace (GCCS) 2017,

> Sebuah ruang siber (cyber) yang bebas, terbuka, dan aman yang didukung oleh hak-hak asasi manusia dan nilai-nilai demokrasi merupakan prasyarat bagi pengembangan sosio-ekonomi. Untuk tujuan inilah, kita harus menyadari bahwa orang/manusia berada di pusat semua kemajuan teknologi. Oleh karena itu kebijakan-kebijakan yang berusaha mengatur teknologi harus berorientasi pada manusia dan pada akhirnya dapat membantu manusia untuk mengembangkan kemampuan mereka sebaik mungkin.
>
> Kami, organisasi dan individu yang bertanda tangan di bawah ini, percaya bahwa agar GCCS 2017 mendukung visi ini, hasilnya harus:

1. Memperkuat prinsip bahwa kebijakan keamanan di dunia maya sejak awalnya harus menghormati hak-hak dan konsisten dengan hukum internasional dan instrumen hak asasi manusia internasional.
2. Mempromosikan dan berkomitmen pada pendekatan multi-stakeholder dalam pengembangan kebijakan siber di tingkat nasional, regional, dan internasional
3. Meningkatkan kolaborasi yang lebih besar lagi dan lebih inklusif di bidang pengembangan kapasitas

Selain itu, sehubungan dengan tema konferensi yang spesifik, forum ini harus mencerminkan beberapa hal berikut:

SIber untuk Pertumbuhan

- Akses yang bermanfaat untuk semua orang ke internet yang terbuka adalah fondasi dasar bagi inisiatif pertumbuhan dan tata kelola di dunia maya. Akses tanpa hambatan, tanpa gangguan, terjangkau, dan netral ke internet akan mendorong inovasi, memberikan pengguna lebih banyak pilihan, dan menjadikan jaringan dan layanan digital lebih kuat. Gangguan jaringan akan memperlambat upaya untuk membangun perekonomian digital secara berkelanjutan dan membatasi akses terhadap layanan-layanan digital yang penting.
- Perkembangan ekonomi digital bergantung pada kebijakan dan peraturan, karena itu perlu dibangun di atas kerangka hukum yang dapat menjamin bahwa orang-orang memiliki kendali atas data mereka dan dapat mempercayai entitas publik dan swasta dimana mereka berinteraksi secara online.
- Perekonomian digital tumbuh subur saat pengguna menciptakan dan berinovasi, usaha-usaha kecil berhasil dan pengusaha menciptakan produk dan layanan yang dapat mengatasi tantangan lokal. Akses terhadap modal, perangkat lunak gratis dan open source (free and open source software / FOSS), dan jaringan komunitas hanyalah beberapa pondasi dasar penting dari perekonomian digital lokal.
- Kemampuan individu untuk berpartisipasi penuh dalam perekonomian digital membutuhkan sebuah akses Internet yang terbuka, dapat diandalkan dan terpercaya, serta ketersediaan dan aksesibilitas terhadap alat, dan pelatihan untuk memastikan keamanan dan privasi online mereka.

Siber untuk Digital Inklusi

- Pendekatan yang terbuka, transparan, dan inklusif terhadap pembuatan kebijakan siber adalah cara terbaik untuk mendorong dan memastikan dunia maya yang inklusif bagi semua orang.
  Menjembatani kesenjangan digital antara dan di dalam negara melalui akses yang bermanfaat merupakan prasyarat bagi semua warga negara untuk memperoleh manfaat sepenuhnya dari perekonomian digital. Memastikan akses yang baik, tidak hanya akses ke infrastruktur, namun juga akses ke Internet yang bebas, terbuka, terjangkau dan aman
- --termasuk peningkatan literasi digital untuk semua orang-- merupakan kunci penting untuk digital inklusi dan pemenuhan hak asasi manusia sepenuhnya.
  Digital inklusi (penggunaan internet untuk kepentingan ekonomi dan bisnis) harus didukung dengan upaya pengembangan kapasitas
- yang disesuaikan dengan kebutuhan yang diinginkan masyarakat dan komunitas secara spesifik agar mendapatkan keuntungan.

Siber untuk Keamanan

- Pengembangan dan implementasi undang-undang, kebijakan, dan praktik yang terkait dengan keamanan siber (cybersecurity) harus berpusat pada orang dan konsisten dengan hukum internasional, termasuk hukum hak asasi manusia internasional.
- Promosi keamanan, stabilitas dan ketahanan dunia maya merupakan tanggung jawab bersama dan harus mencakup semua pemangku kepentingan. Selain itu kemitraan antara publik dan swasta juga penting dilakukan, kerangka kerjasama ini perlu dibuat transparan dan akuntabel.
- Penggunaan teknologi apapun yang digunakan untuk memantau dan mengendalikan konten harus ditentukan oleh undang-undang. Ini diperlukan untuk mencapai tujuan yang sah dan sesuai dengan tujuan yang dikejar, sebagaimana didefinisikan secara jelas dalam General Comment 34 of the Human Rights Committee and the Internasional Principles mengenai Penerapan Hak Asasi Manusia terhadap Pengawasan Komunikasi.
- Standar perilaku online harus dirancang agar berpusat pada orang dan menghargai hak-hak, dan dikembangkan secara terbuka, transparan, dan inklusif.
- Pengembangan kapasitas keamanan siber memiliki peranan penting dalam meningkatkan keamanan setiap orang baik online maupun offline. Upaya tersebut harus mempromosikan pendekatan yang menghormati hak asasi manusia terhadap keamanan dunia maya.

Siber untuk Diplomasi

- Peran integral dan potensi dari TIK dan dunia maya untuk mempromosikan perdamaian dan keamanan harus terus dieksplorasi dan dipromosikan.
- Hukum dan standar internasional yang berlaku saat ini harus sesuai untuk dunia maya dan harus dikembangkan untuk menghadapi berbagai tantangan yang muncul.
- Pengembangan dan kerjasama kebijakan internasional yang berhubungan dengan ruang siber harus dibuat inklusif dan transparan, serta secara konsisten mematuhi aturan hukum.
- Setiap negara harus mematuhi norma-norma perilaku yang ada di negara tersebut dan disesuaikan dengan hukum hak asasi manusia internasional yang mempromosikan internet bebas dan terbuka.

Kami ingin menekankan bahwa upaya baru apapun yang terkait dengan pengembangan kapasitas siber dan inisiatif untuk membagikan informasi dan pengetahuan harus berupaya membangun dan melengkapi proses dan forum yang sudah ada (seperti Global Forum on Cyber Expertise). Mereka harus terbuka, transparan, dan inklusif terhadap semua pemangku kepentingan, konsensus, dan akuntabel. Mereka harus memfasilitasi sharing keahlian dan praktik yang baik, berkomitmen untuk menangani kesenjangan digital, dan perlu untuk membangun kapasitas dari semua pemangku kepentingan, khususnya di negara-negara berkembang.

Proses dalam GCCS adalah sebuah platform penting untuk mencapai visi-visi di atas. Kami berharap ini berlanjut menjadi proses multi-stakeholder yang sesungguhnya, termasuk partisipasi dari masyarakat sipil. Perspektif gender dan prinsip keseimbangan seharusnya diperhitungkan, sehingga partisipasi dari semua pemangku kepentingan dapat bermanfaat.

Yang menandatangani:

ORGANISASI

1. Association for Progressive Communications.
2. Institute for Policy Research and Advocacy (ELSAM) Indonesia.
3. Collaboration on International ICT Policy in East and Southern Africa (CIPESA).
4. Kenya ICT Action Network (KICTANet).
5. Access Now.
6. ICT Watch, Indonesia.
7. Derechos Digitales, Chile.
8. Persatuan Kesedaran Komuniti Selangor (EMPOWER), Malaysia.
9. Red en Defensa de los Derechos Digitales, Mexico.
10. Karisma Foundation, Colombia.
11. Digital Empowerment Foundation, India.
12. Sinar Project, Malaysia.
13. Human Rights Online Philippines.
14. Forum for Digital Equality.
15. TEDIC, Paraguay.
16. Rudi International, Democratic Republic of Congo.
17. Paradigm Initiative, Nigeria.
18. Global Partners Digital, UK.

B. **Keselarasan Kewajiban dan Tanggung Jawab Hukum**

Lanskap hukum cybersecurity masih dapat dikatakan kosong. Sampai hari ini, masih belum terdapat suatu kerangka global yang disepakati bersama untuk perlindungan data. Tidak ada koherensi untuk proses berbagi informasi antara entitas sektor swasta dan publik untuk mewujudkan tujuan cybersecurity dan juga keamanan nasional dan penegakan hukum. Bagi organisasi global yang beroperasi di berbagai pasar, faktor-faktor ini semakin menghambat pengadopsian dan pelaksanaan strategi-strategi cybersecurity.

Tidak adanya perjanjian global dan khususnya trans-Atlantik tentang standar-standar perlindungan data mulai disoroti setelah adanya keputusan Court of Justice of the European Union in Schrems v Dat Protection Commissioiner on the Safe Harbour Agreement pada 2015. Kasus ini membatalkan dasar hukum yang mengizinkan perusahaan untuk mentransfer data yang dikumpulkan di wilayah Uni Eropa (UE) ke Amerika Serikat (AS) untuk diproses.

Keputusan ini sebenarnya didasarkan pada pertanyaan-pertanyaan terkait ketimpangan antara perlindungan data dan privasi di UE dan AS, namun keputusan tersebut berdampak global. Seiring semakin banyaknya perusahaan di Eropa yang berusaha mengalihdayakan proses bisnis mereka ke negara-negara di luar Eropa, rezim privasi dan perlindungan data di Asia, Amerika Latin dan Afrika akan semakin menstandarisasi kerangka regulasi kerjasama mereka dengan Eropa.

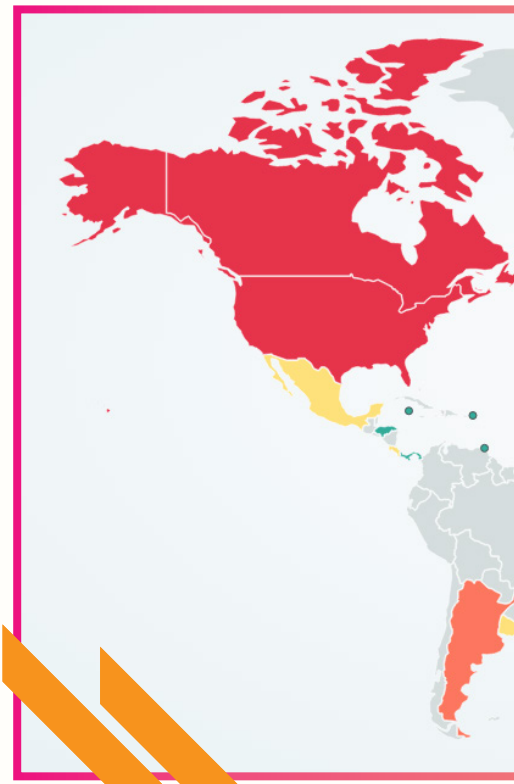
Menyusul keputusan Court of Justice, UE dan AS memulai proses pengadopsian penerus perjanjian tersebut, yaitu Privacy Shield. Namun, sejauh ini masih belum terdapat suatu solusi jangka panjang terhadap ketimpangan pendekatan perlindungan data. Eropa sejak lama telah menjalankan pendekatan regulasi aktif untuk melindungi data pribadi, sementara AS lebih memilih rezim regulasi diri maupun sektoral. Hal ini menimbulkan banyak kebingungan bagi perusahaan-perusahaan yang beroperasi di kedua yurisdiksi tersebut.

> Perusahaan swasta juga kewalahan dengan banyaknya standar di sejumlah area, sementara amat kekurangan standar di area yang lain.

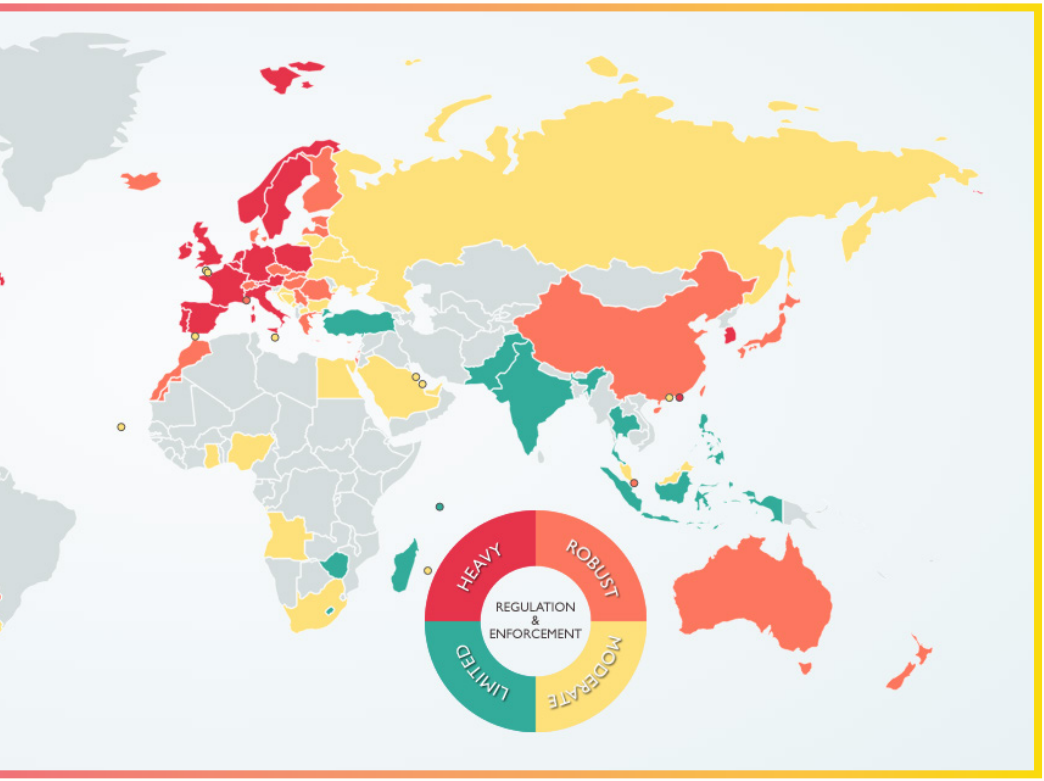
Seiring bertambahnya jumlah perusahaan yang beroperasi lintas negara, dan semakin banyaknya negara-negara di seluruh dunia yang mengadopsi legislasi yang meniru pendekatan UE tersebut, kepentingan bisnis untuk mewujudkan perjanjian global untuk perlindungan data menjadi semakin kuat. UE dan AS mencapai kesepakatan payung yang bernama Umbrella Agreement on Data Protection pada September 2015, yang dirancang untuk diberlakukan pada transfer data trans-Atlantik antara lembaga pemerintah (bukan dengan perusahaan), yang menjadi langkah awal untuk melakukan standarisasi kedua rezim tersebut.

C. **Peta Regulasi Perlindungan Data di Seluruh Dunia**

Terdapat lebih dari 1000 publikasi yang berupaya menetapkan standar-standar teknis tentang cybersecurity, namun belum ada satu pun yang secara komprehensif membahasnya. Hal ini menyebabkan terjadinya ketimpangan dan perpecahan dalam perkembangan standar teknis. Sebuah laporan US National Institute of Standards and Technology (NIST) pada Desember 2015, yang mengidentifikasi sepuluh area inti standarisasi cybersecurity (termasuk misalnya teknik kriptografi) menyatakan bahwa dari seluruh aplikasi kunci yang ada seperti cloud computing, manajemen darurat atau manajemen pemungutan suara, standar yang ada masih bersifat parsial, sama sekali tidak ada atau masih dikembangkan di berbagai area. Standar-standar teknis tersedia hanya pada sejumlah area standarisasi, seperti keamanan jaringan untuk aplikasi pemungutan suara.



Peta ini dirilis oleh DLA Piper pada 2012, dan diperbarui setiap tahun. Isu privasi muncul seiring dengan tumbuhnya pengguna teknologi mobile. Makin banyaknya aliran data di seantero dunia telah mendorong negara-negara untuk mengadopsi regulasi perlindungan data yang baru, dan menciptakan kemungkinan perlindungan yang lebih luas bagi pengguna data. Peta interaktif ini dapat diakses di http://s.id/PRo.



Peta Regulasi Perlindungan Data Dunia (Sumber: http://dataprivacysite.com)

D. Praktik Berbagi Informasi

Pada 2015, AS dan Eropa mengadopsi legislasi terkait pembukaan informasi oleh enttas perusahaan dan antar lembaga pemerintah untuk tujuan cybersecurity. US Cybersecurity Information Sharing Act (CISA), yang disahkan menjadi undang-undang pada Desember 2015, mengizinkan perusahaan internet dan entitas sektor swasta lain di AS untuk membagi informasi lalu lintas internet kepada Pemerintah AS, khususnya dalam kondisi adanya ancaman cybersecurity. Undang-Undang tersebut telah menuai kritik keras dari para pejuang HAM dan organisasi masyarakat sipil yang mengkhawatirkan undang-undang tersebut dimanfaatkan untuk memberikan kekebalan bagi perusahaan dari gugatan perdata dan tuntutan pidana jika membagi informasi pribadi seseorang meskipun tanpa surat perintah.

Undang-Undang ini mengizinkan data dibagi kepada berbagai lembaga pemerintah, dari FBI dan NSA hingga Internal Revenue Service. Dalam suatu lingkungan yang telah dipenuhi masalah akuntabilitas dan transparansi lembaga-lembaga intelijen AS, banyak yang khawatir CISA akan digunakan sebagai salah satu alat pengawasan (pengawasan) baru. Namun, pemerintah berpendapat bahwa CISA diperlukan untuk mendorong entitas perusahaan untuk berbagi data yang penting untuk mendeteksi dan mencegah ancaman cybersecurity.

Pada bulan yang sama ketika CISA disahkan, UE membuat perjanjian tentang Network and Information Security (NIS) Directive. Panduan atau Directive ini tidak hanya mengharuskan disusunnya suatu strategi cybersecurity nasional, namun juga mewajibkan operator layanan-layanan vital (seperti layanan transportasi atau keuangan) dan penyedia layanan digital untuk melaporkan insiden cybersecurity kepada pihak berwenang nasional. Kedua inisiatif baru ini menandai munculnya era baru regulasi yang mewajibkan untuk melaporkan dan merespon insiden terkait cybersecurity.

PERJANJIAN LIMA MATA (THE FIVE EYES AGREEMENT)

Polisi pada umumnya harus menjalani proses formal dan legal – yang seringkali merepotkan - untuk mendapatkan informasi dari dan berbagi informasi dengan kepolisian negara lain di seluruh dunia. Berbeda dengan kepolisian, lembaga intelijen umumnya memiliki hubungan yang lebih cair dan terintegrasi dengan lembaga intelijen lain di seluruh dunia. Hal ini setidaknya terbukti dalam konteks lembaga intelijen AS, Inggris, Australia, Selandia Baru dan Kanada, yang beroperasi dalam suatu aliansi yang disebut sebagai The Five Eyes.

Perjanjian Five Eyes ini didasarkan pada berbagai memorandum kesepahaman multilateral dan bilateral yang bermula pada tahun 1946, yang memudahkan lembaga intelijen di kelima negara tersebut beroperasi dengan cara amat terpadu, mengizinkan mereka berbagi berbagai data pengawasan mentah, melakukan operasi mata-mata dan peretasan bersama, bahkan menempatkan staf di fasilitas satu sama lain.

Setelah terjadinya pembocoran dokumen rahasia oleh seorang whistleblower NSA, Edward Snowden, Five Eyes Agreement ini kemudian menjadi sorotan. Namun, pertukaran informasi intelijen masih tetap berjalan dalam kerahasiaan, dan ditutup-tutupi dari perhatian publik. Organisasi seperti Privacy International telah berulang kali menyerukan dibukanya perjanjian intelijen kepada publik sepenuhnya, dan itu berarti bukan hanya Five Eyes Agreement, namun juga berbagai perjanjian serupa lainnya di seluruh dunia.

E. **Transfer Data Lintas Negara**

Area kebijakan final yang membicarakan keselarasan/koherensi pembagian informasi adalah yang terkait dengan transfer data lintas negara untuk tujuan penegakan hukum dan intelijen. Ini merupakan area yang semakin bermasalah dan kompleks dalam bidang keamanan nasional dan penegakan hukum. Sebelumnya, kepolisian dan lembaga intelijen mampu mengakses data yang dimiliki perusahaan (khususnya perusahaan komunikasi) dengan relatif mudah karena perusahaan tersebut berada di yurisdiksi kepolisian/lembaga intelijen tersebut, namun saat ini mayoritas orang menggunakan layanan komunikasi yang berbasis di luar negeri, khususnya di AS.

Untuk memberikan kekuatan kepada surat perintah yang menuntut dibukanya akses kepada data perusahaan, pemerintah saat ini harus bergantung pada sejumlah Perjanjian bantuan Hukum Bersama (Mutual Legal Assistance Treaties/ MLATS) bilateral dan juga perjanjian intelijen seperti Five Eyes Agreement (lihat halaman 45). Hal ini tidak hanya menghambat efisiensi investigasi, mengingat sebagian besar permintaan yang melalui proses MLAT akan memakan waktu hingga satu tahun, namun juga memberikan insentif bagi pemerintah/negara untuk menyiasati proses tersebut dengan menggunakan intersepsi dan teknik pengawasan lainnya.

The Council of Europe Convention on Cybercrime (Budapest Convention, lihat halaman 58) berisi ketentuan-ketentuan yang mengizinkan para pihak untuk mendapatkan akses lintas-negara kepada data komputer dengan izin atau selama memang tersedia untuk publik (Pasal 32). Ketentuan ini dirancang untuk memungkinkan akses unilateral oleh satu pihak kepada data yang dimiliki di yurisdiksi pihak lain, dan karenanya merupakan suatu jalan pintas atau pengecualian terhadap proses MLAT. Pertanyaan mengenai akses lintas-batas adalah suatu isu yang amat kontroversial, antara lain karena Pasal 32 dapat ditafsirkan sebagai izin untuk melakukan pencarian jarak jauh dan penyitaan (yang disebut juga sebagai intrusi atau peretasan), dan dijadikan oleh negara seperti Rusia sebagai alasan untuk tidak bergabung dalam Konvensi tersebut, karena dianggap melanggar prinsip kedaulatan.

Pada 2013, Council of Europe mengusulkan suatu protokol tambahan untuk Convention on Cybercrime terkait akses data lintas-negara, namun kemudian memutuskan bahwa usulan tersebut tidak dapat dilaksanakan. Dalam bulan-bulan setelahnya, pembocoran data oleh Snowden terkait pengawasan yang dilakukan AS dan Inggris diterbitkan, dan mentransformasi debat terkait penegakan hukum dan akses intelijen kepada data pribadi. Sebuah laporan tahun 2013 yang disusun oleh Cybercrime Convention Committee, sub-grup yurisdiksi dan akses lintas negara kepada data menyatakan bahwa berbagai perkembangan terbaru juga mengharuskan dilakukannya revisi terhadap Pasal 32b, dan menegaskan bahwa ”praktik saat ini terkait penegakan hukum langsung dalam hal akses kepada data […] seringkali melampaui batasan yang dinyatakan dalam Pasal 32b dan Budapest Convention secara umum,” yang rentan berdampak negatif pada penegakan HAM.

Setiap negara berkepentingan untuk mendukung pengembangan kapasitas pemerintah negara lain untuk mendeteksi dan merespon ancaman cybersecurity.

GERAK TANGKAS MULTISTAKEHOLDER INDONESIA ATASI RANSOMWARE WANACRY

Ancaman datangnya ransomware WannaCry pada Mei 2017 tidak main-main. Pertengahan Maret 2017, dua rumah sakit di Indonesia terkena imbas serangan ransomware WannaCry. RS Harapan Kita dan RS Dharmais jadi korban virus yang mengganggu sistem komputer, sehingga layanan medis ikut terbengkalai. Untuk menangkal penyebaran serangan, tentu saja Kementrian Komunikasi dan Informatika (Kemkominfo) tak dapat bekerja sendirian.

Sejumlah multistakeholder seperti akademisi, pakar, teknisi, pebisnis, instansi pemerintah, aktivis, hingga media, segera membentuk tim darurat demi menangani ransomware yang bisa melumpuhkan jaringan komputer itu. Menteri Komunikasi dan Informatika (Menkominfo) Rudiantara beserta segenap kalangan tadi berinteraksi secara aktif di WhatsApp (WA) Group. Setiap anggota saling menawarkan bantuan sesuai dengan kemampuan dan kompetensinya masing-masing. Dalam WA Group tersebut terjadi diskusi yang luar biasa aktif, mulai dari informasi penyebaran ransomware, apa dampaknya, seberapa besar kerugian, bagaimana cara penanganannya, hingga menyosialisasikannya. Berkat kekompakan semua multistakeholder, Kemenkominfo dapat segera merilis sejumlah kampanye yang disebarluaskan media mengenai bahaya ransomware dan langkah antisipasinya.

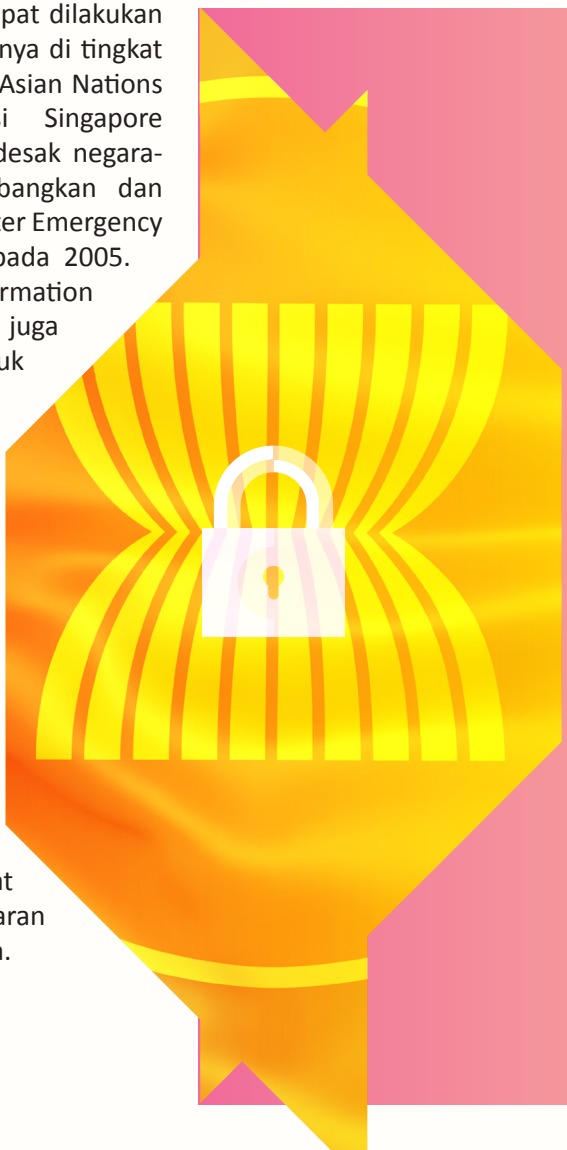
Diskusi seru di WA Group tersebut akhirnya melahirkan suatu acara jumpa pers pada 14 Mei 2017 di sebuah kafe di bilangan Cikini, Jakarta Pusat. Walau saat itu hari Minggu yang semestinya hari libur, namun Menkominfo Rudiantara bersama pihak terkait seperti ID-SIRTII dan ICT Watch meluangkan waktu untuk memberi penjelasan terkait penanganan ransomware WannaCry. Dengan sangat gamblang, Rudiantara mempresentasikan langkah-langkah yang dapat dilakukan pengguna internet untuk menghadapi serangan tersebut. Adi Jaelani dari ID-SIRTII ikut menjelaskan langkah teknis yang lebih detil. Menurutnya, sebaiknya backup dilakukan melalui sistem operasi Linux atau Ubuntu. Seperti kita tahu, WannaCry memang hanya menarget sistem operasi Microsoft Windows, sehingga paling ideal adalah melakukan backup di sistem operasi selain Windows.

Sebelumnya, sudah beredar pula pers rilis dari Kemkominfo pada 13 Mei 2017 yang disebar ke seluruh media massa. Pers rilis itu berisi serangkaian petunjuk teknis mengantisipasi serangan ransomware, baik sebelum maupun sesudah diserang. Dilansir Kompas.Com, pihak Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII) menyebut jumlah komputer milik rumah sakit di dalam negeri yang terserang ransomware WannaCry mencapai ratusan unit.

Pihak Id-SIRTII membuka konsultasi secara online bagi semua warganet yang membutuhkan di https://www.nomoreransom.org . Mereka juga menerima berbagai keluhan di email incident@idsirtii.or.id. Laman situs Kominfo.go.id pun memuat beragam petunjuk pencegahan dan penanganan apabila terjadi insiden.

Pendidikan nasional dan program peningkatan kesadaran publik amat penting untuk mendidik setiap orang mengenai cybersecurity

Pembangunan kapasitas cybersecurity merupakan suatu area di mana dapat dilakukan kerja sama yang signifikan, khususnya di tingkat regional. Association of Southeast Asian Nations (ASEAN) misalnya, mengadopsi Singapore Declaration pada 2003 yang mendesak negara-negara anggota untuk mengembangkan dan mengoperasionalkan suatu Computer Emergency Response Team (CERT) nasional pada 2005. Selain itu, EU Networks and Information Security (NIS) Directive yang baru juga mewajibkan negara anggota untuk mengadopsi strategi NIS nasional yang menetapkan sasaran strategis dan kebijakan dan upaya regulasi yang sesuai dalam hal cybersecurity.



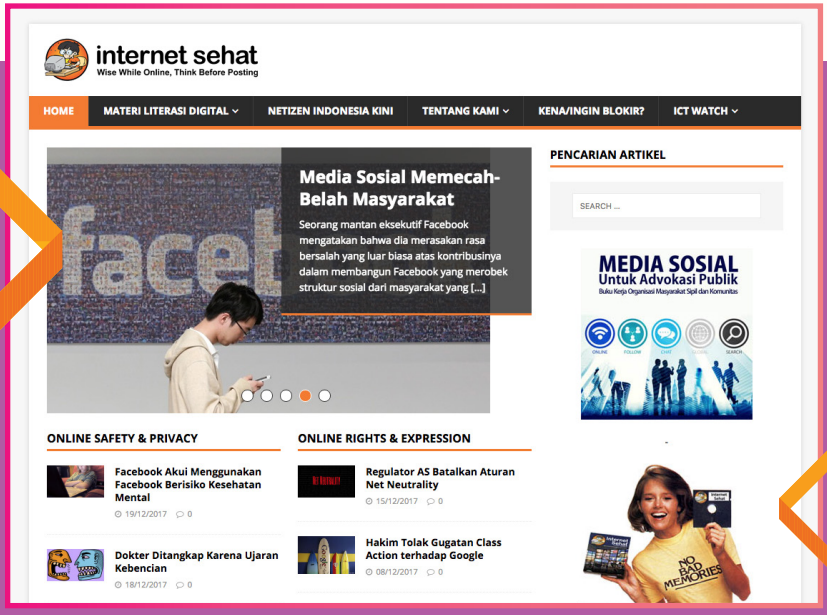
Negara-negara anggota juga akan diwajibkan untuk menetapkan suatu lembaga kompeten nasional untuk melaksanakan dan menegakkan Directive tersebut, serta menetapkan Tim CSIRT yang bertanggung jawab menangani insiden dan risiko. UE juga melakukan pelatihan darurat dan menyelenggarakan hari kesadaran cybersecurity di seluruh wilayahnya.

INTERNET SEHAT, PROGRAM LITERASI DIGITAL DARI ICT WATCH

ICT Watch berkomitmen terhadap kebebasan berekspresi di Internet dan menyadari tantangan-tantangan yang muncul, sambil terus memerangi hoax, ujaran kebencian dan disinformasi di Internet dengan menjalankan gerakan literasi digital Indonesia, yang disebut "Internet Sehat", kepada publik. Internet Sehat menyediakan konten online berbahasa Indonesia yang berkualitas dengan lisensi creative-common, berupa:

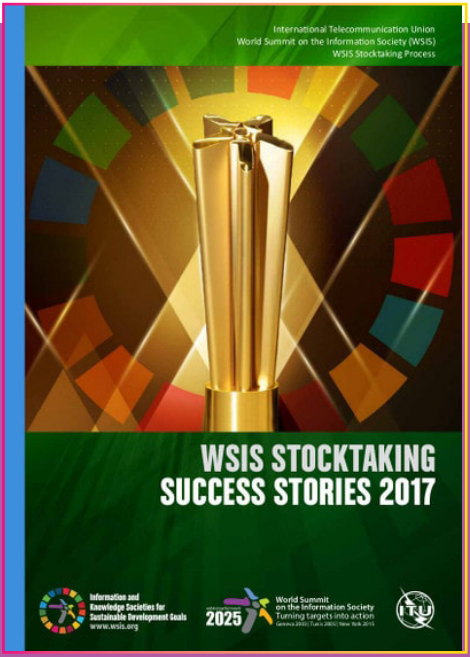
a). Seri film dokumenter tentang peran media sosial dalam gerakan sosial dengan subtitle berbahasa Inggris (**http://lenteramaya.ictwatch.id**) untuk kegiatan pemutaran film / diskusi publik, dan
b). Kit presentasi dan modul how-to yang telah diperbarui (**http://internetsehat.id/literasi**) untuk edukasi / advokasi publik.

Pesan kunci Internet Sehat juga disampaikan melalui berbagai kegiatan offline, seperti workshop / roadshow ke sekolah-sekolah, kampus dan masyarakat lokal, sekaligus memfasilitasi keterlibatan multistakeholder dan pengembangan kapasitas aktor/komunitas lokal. Melalui beberapa saluran online, Internet Sehat juga memanfaatkan media sosial (statistik per 15 Februari 2017): Facebook Page (73.340 Likes) **http://facebook.com/netsehat** (terverifikasi), Twitter (824 ribu follower) **http://twitter.com/internetsehat** (terverifikasi), YouTube (**http://youtube.com/internetsehat**), SlideShare (**http://slideshare.net/internetsehat**) dan Flickr (**http://flickr.com/internetsehat**).



ICT Watch sendiri adalah Organisasi Masyarakat Sipil (OMS) yang didirikan untuk mengembangkan, memberdayakan dan mendukung orang, organisasi masyarakat sipil dan para pemangku kepentingan lainnya di Indonesia untuk mendapatkan hak atas informasi. ICT Watch percaya bahwa Internet merupakan salah satu alat yang paling ampuh untuk memfasilitasi keterlibatan warga dalam membangun masyarakat yang demokratis dan mempromosikan berbagai hak asasi manusia. Oleh karena itu, ICT Watch memberikan informasi tentang dinamika dan manfaat potensial Internet melalui kampanye, publikasi dan berbagai variasi kegiatan publik. ICT Watch secara tegas menentang kebijakan yang tidak jelas yang mengganggu penyensoran di Internet, dan melindungi akses terhadap informasi bagi masyarakat. Selanjutnya, hal ini akan merangsang penggunaan internet yang aman dan bijaksana di Indonesia.

Internet Sehat adalah sebuah gerakan advokasi literasi digital yang diinisasi pada tahun 2002 dan terus dijalankan secara konsisten oleh ICT Watch hingga saat ini di berbagai daerah di seluruh Indonesia. Pada Mei 2016 di Jenewa, ICT Watch mendapatkan sebuah pencapaian internasional, The World Summit on the Information Society (WSIS) Champion, dari Perserikatan Bangsa-Bangsa (PBB) - Internatonal Telecommunica on Union (ITU). Tahun 2017, ICT Watch menjadi 1st Winner untuk kategori Ethical Dimensions of the Information Society. PBB / ITU menilai bahwa program Internet Sehat merupakan salah satu model strategi advokasi tentang etika online dan literasi digital untuk masyarakat.



Melalui program Internet Sehat, ICT Watch berupaya menunjukkan kepada pemerintah bahwa masyarakat dapat bertanggung jawab atas kegiatan online mereka. Untuk itu Internet Sehat memperkenalkan modul how-to bagi para orangtua dan guru tentang pengetahuan dasar internet, bahaya internet, serta literasi informasi, keamanan dan perlindungan privasi. Modul-modul ini dipatenkan di bawah lisensi creative-common, dan telah digunakan oleh organisasi lain dalam berbagai pelatihan keterampilan internet.

Internet Sehat juga menyelenggarakan berbagai kegiatan offline, seperti workshop dan pelatihan, acara publik, roadshow ke ribuan sekolah, kampus dan komunitas. Internet Sehat juga menyediakan konsultasi secara online dan kampanye mengenai “etika berinternet yang baik” dengan menggunakan semua media yang tersedia (misalnya situs web, Twitter, Facebook, dan sebagainya). Dua sampai tiga tips dan trik tentang “cara menggunakan Internet dengan aman dan bijak” juga di-posting setiap hari melalui media sosial kami. Internet Sehat juga menyediakan “Tanya Jawab” melalui media sosial maupun media online.

Sebelumnya pada Agustus 2014 di Jakarta, ICT Watch juga telah mendapatkan pengakuan nasional berupa Tasrif Award dari Aliansi Jurnalis Independen (AJI) Indonesia. AJI berpendapat bahwa ICT Watch, melalui program Internet Sehat, telah menjalankan peran yang penting dalam demokratisasi Internet serta mempromosikan Internet sebagai media pemenuhan hak warga negara atas informasi. Dalam menjalankan kegiatan dan program Internet Sehat, ICT Watch selalu berkolaborasi dengan berbagai multistakeholder. ICT Watch juga merupakan salah satu perintis dan pegiat untuk beberapa inisiatif, seperti Southeast Asia Freedom of Expression Network (SAFEnet), Indonesian CSOs Network for Internet Governance (ID-CONFIG), Indonesia Internet Governance Forum (ID-IGF) dan Indonesia Child Online Protection (ID-COP).

Semangat Internet Sehat adalah sebagai berikut:

"Untuk mempromosikan kebebasan berekspresi di internet secara aman dan bijaksana, melalui beberapa pendekatan berikut: 1) Konten online yang positif, bermanfaat dan menarik harus dikembangkan dari-oleh-untuk anak-anak, remaja dan masyarakat lokal, 2) Inisiatif self-filtering di internet hanya dapat dilakukan di level keluarga (rumah) dan pendidikan (sekolah), dan 3) Literasi digital dan perlindungan online anak sangat membutuhkan dialog dan kerjasama multistakeholder yang inklusif, setara, transparan dan akuntabel dalam koridor Internet Governance."

Sebenarnya ICT Watch tidak mau mengklaim kepemilikan gerakan advokasi Intenet Sehat yang sudah banyak diadopsi di masyarakat. Sebaliknya, ICT Watch tidak ingin Internet Sehat diklaim oleh individu dan / atau institusi tertentu sebagai pencapaiannya, terutama jika cenderung dikomersilkan. Itulah sebabnya nama "Internet Sehat" sebagai objek hak kekayaan intelektual telah didaftarkan secara resmi oleh ICT Watch di bawah Direktorat Jenderal Hak Kekayaan Intelektual, Kementerian Kehakiman dan Hak Asasi Manusia, sejak Oktober 2010. Namun untuk penggunaan oleh publik, Internet Sehat menggunakan lisensi creative-commons: Attribution - Non Commercial - Share Alike (CC BY-NC-SA), dimana lisensi tersebut memungkinkan orang lain untuk mendesain ulang dan menyesuaikan kontennya untuk kepentingan non-komersial, selama mereka memberikan kredit dan lisensi kreasi baru mereka di bawah aturan yang identik.

Baru-baru ini, bersama dengan Kementerian Komunikasi dan Informatika Indonesia, UNICEF, Universitas Indonesia (UI) dan Komisi Perlindungan Anak Nasional (KPAI), saat ini ICT Watch sedang dalam tahap pengembangan akhir menyusun Roadmap Perlindungan Anak Nasional.

Visi ICT Watch

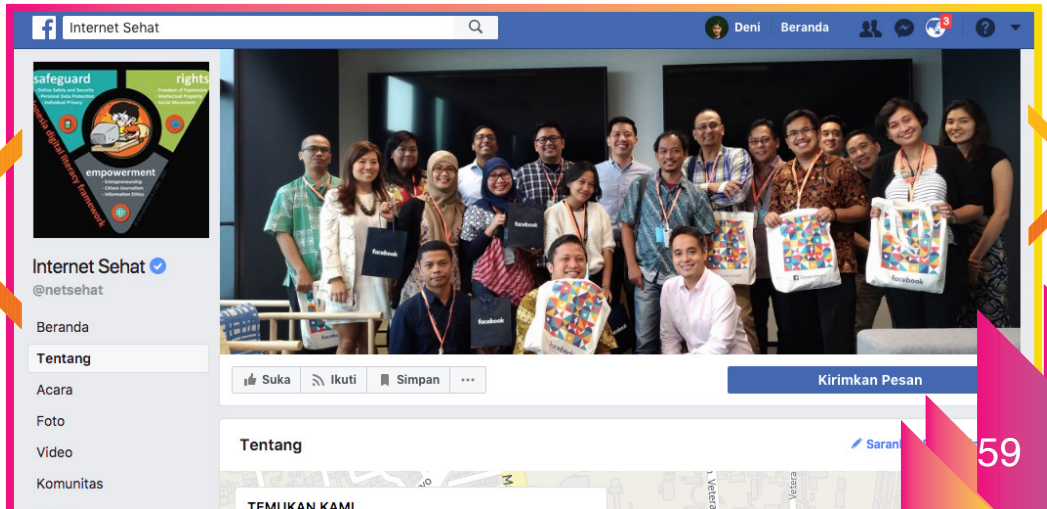
"Mewujudkan terbentuknya ekosistem tata kelola Internet yang melindungi dan memenuhi hak warga negara terhadap informasi dan kebebasan berekspresi, serta pemanfaatan Teknologi Informasi dan Komunikasi (TIK), termasuk Internet, sebagaimana diamanatkan oleh Konstitusi Indonesia".

Adapun Misi ICT Watch

Mengembangkan kesadaran masyarakat Indonesia, penekanan pada anak-anak dan keluarga, tentang penggunaan TIK dan Internet dengan aman dan bijaksana. (INTERNET SAFETY)

Memberdayakan masyarakat sipil Indonesia, terutama para aktivis informasi dan hak asasi manusia, dengan mendukung mereka untuk menggunakan TIK dan Internet karena mereka adalah alat yang memungkinkan dalam memenuhi hak atas informasi. (INTERNET RIGHTS).

Untuk mendukung dialog multi-pihak Indonesia dalam ICT dan Internet Governance sambil menjunjung prinsip-prinsip kunci transparansi, akuntabilitas, kesetaraan, kolaborasi dan profesionalisme. (INTERNET GOVERNANCE)



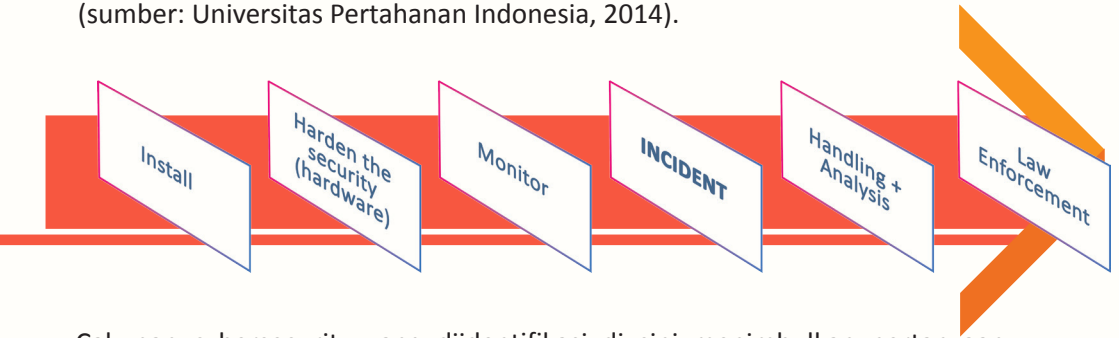
BAB III

Kilas Kebijakan Cybersecurity Indonesia

A. Kilas Tata Kelola Cybersecurity Indonesia

Terjadinya Reformasi 1998 menandai suatu titik balik utama dalam sejarah media di Indonesia. Perubahan lanskap media bersamaan dengan kemajuan inovasi teknolgi menciptakan kebutuhan regulasi di sektor tersebut. Namun, kebijakan-kebijakan yang kemudian muncul terkadang tidak memahami konteks di mana teknologi baru bekerja, dan karenanya gagal mengantisipasi konsekuensinya. Serupa dengan itu, pesatnya perkembangan internet tidak selalu ditanggapi dengan kebijakan yang tepat. Salah satu tantangan baru atas perluasan inovasi teknologi baru ini adalah cybersecurity.

Menyusul putaran terakhir mengenai isu cybersecurity, para pemangku kepentingan telah merespon dengan mengembangkan suatu mekanisme untuk melindungi dan meminimalkan gangguan terhadap kerahasiaan, integritas dan ketersediaan informasi. Dalam konteks Indonesia, mekanisme ini berjalan dari tahap instalasi, setup hardware, hingga proses pemantauan dan penegakan hukum. Gambar berikut menunjukkan cakupan cybersecurity di Indonesia (sumber: Universitas Pertahanan Indonesia, 2014).



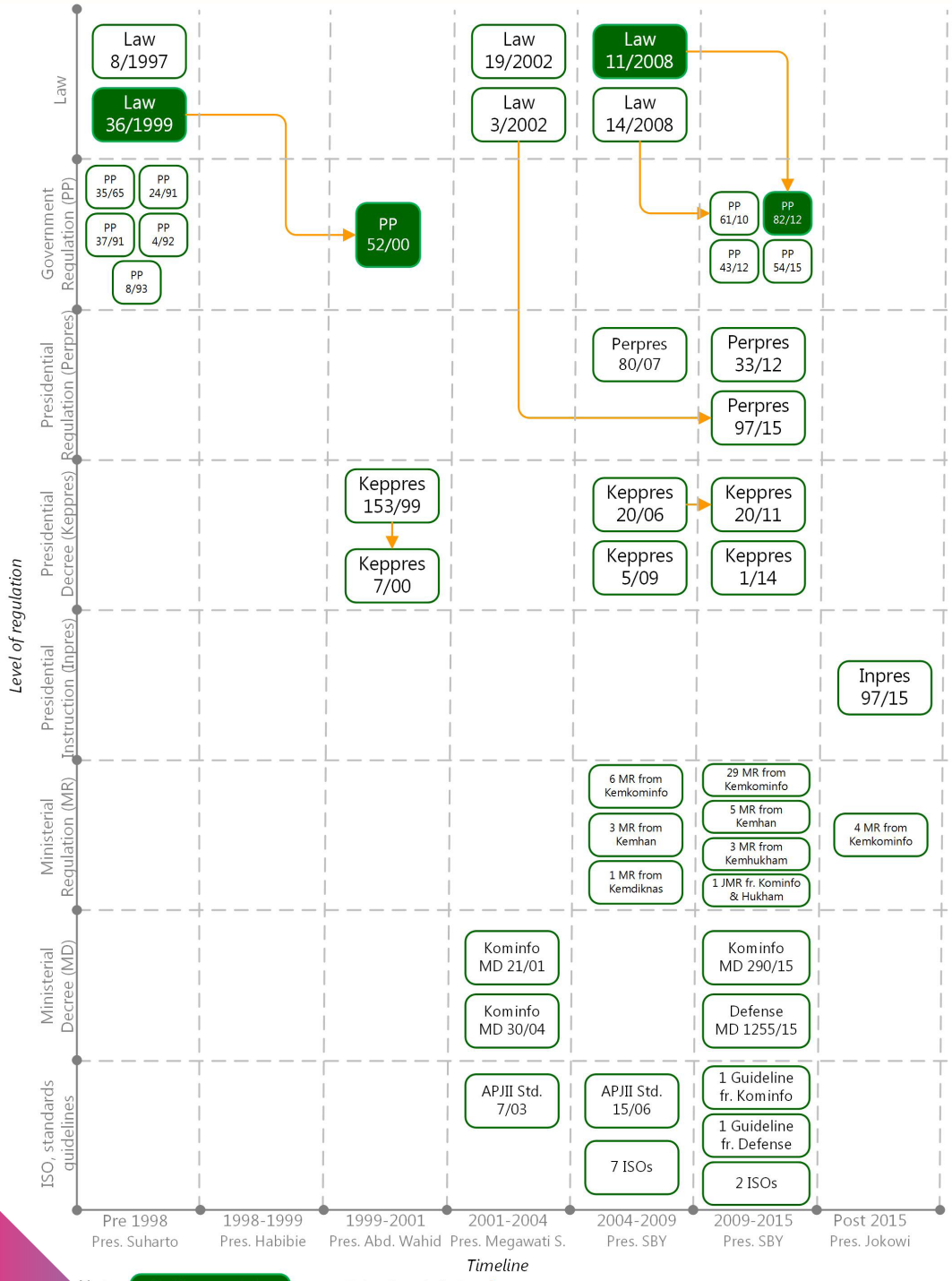
Cakupan cybersecurity yang diidentifikasi di sini menimbulkan pertanyaan seputar kebijakan. Sejauh ini telah ada beberapa pertanyaan terkait apakah pemerintah akan bertanggung jawab sendiri terhadap seluruh cakupan cybersecurity. Sejauh ini kami menemukan bahwa kebijakan (atau tidak adanya kebijakan) mempengaruhi dinamika cybersecurity, yang pada gilirannya juga akan berdampak pada masyarakat.

Setelah mengkaji berbagai peraturan yang ada tentang cybersecurity di Indonesia, ditemukan bahwa dasar hukum cybersecurity masih lemah. Dibandingkan dengan negara lain, Indonesia masih tertinggal dalam hal kebijakan dan peraturan keamanan TIK. Padahal Malaysia misalnya, telah memiliki Undang-Undang Kejahatan Komputer (Computer Crime Act), UU Tanda Tangan Digital (Digital Signature Act), UU Telemedicine (ketiganya disahkan sejak 1997), UU Multimedia (1998), UU Sistem Pembayaran (2003), dan UU Data Pribadi (2010). Sementara itu Singapura juga memiliki sejumlah peraturan sejenis. Kurangnya kebijakan di Indonesia adalah satu hal yang sama-sama disepakati oleh semua ahli yang diwawancara dalam penelitian ini, serta diakui secara terbuka oleh para pejabat pemerintah.

Jika sejarah kebijakan cybersecurity di Indonesia diamati secara mendalam, akan terlihat bahwa kebijakan-kebijakan yang ada saat ini berkisar pada dua undang-undang utama, yaitu UU Telekomunikasi No.36/1999 dan UU ITE No.11/2008. UU Telekomunikasi No.36/1999 adalah produk Reformasi, dan telah berkontribusi pada dinamika terakhir di sektor telekomunikasi di Indonesia. Sementara itu UU ITE No.11/2008 merupakan undang-undang cyber pertama Indonesia yang terkenal karena kontroversinya terkait pasal 27 ayat 3 yang sering dimanfaatkan dalam berbagai kasus pidana pencemaran nama baik.

B. **Tantangan Tata Kelola Cybersecurity Indonesia**

Kedua Undang-Undang tersebut memiliki tantangannya masing-masing. UU Telekomunikasi misalnya, meskipun memfasilitasi kompetisi dalam industri telekomunikasi, tidak menyebutkan infrastruktur telekomunikasi dalam konteks internet. Hal ini menyulitkan dalam memasukkan suatu kasus ke dalam konteks yang tepat. Selain itu, meskipun sudah ada legislasi terkait kejahatan cyber yang disahkan, yaitu UU No.11/2008 tentang Internet dan Transaksi Elektronik (Pasal 29-37), cakupannya amat terbatas, karena masih memerlukan dukungan tambahan dari Undang-Undang lain. Karena keterbatasan ini, kasus-kasus pidana terkait kejahatan cyber ditangani dengan UU KUHAP, UU Perlindungan Konsumen No.8/1999, UU Hak Cipta No.19/2002 atau UU Anti-Pornografi No.44/2008.



Peraturan dan standar terkait cybersecurity (Sumber: CIPG 2016)

Keterbatasan kedua UU tersebut telah membuat regulator memahami pentingnya mengeluarkan peraturan teknis sebagai pelengkap khususnya untuk sektor-sektor tertentu. Peraturan teknis yang melengkapi kedua undang-undang tersebut telah dikirimkan oleh Kominfo kepada Kemenko Polhukam dan juga Kepolisian. Pada periode 2009-2015, lebih dari 30 peraturan dan standar diterbitkan untuk menghadapi isu-isu cybersecurity khususnya dari aspek teknis (lihat lampiran untuk perinciannya). Namun mayoritas aktor sepakat bahwa seperangkat peraturan tersebut masih belum cukup, khususnya ketika dihadapkan pada kompleksitas dan pertumbuhan ancaman cyber saat ini. Peraturan terkait e-commerce, merk dagang/domain, privasi dan keamanan online, hak cipta, regulasi konten, penyelesaian sengketa serta infrastruktur kritis TIK adalah beberapa jenis peraturan yang diperlukan.

Dengan menyadari bahwa tata kelola cybersecurity yang efektif memerlukan regulasi, kesadaran dan koordinasi bersama, pemerintah merespon dengan menginisiasi pembentukan Badan Cyber Nasional (BCN) sambil memperbaiki peraturan serta membangun kesadaran nasional di saat yang sama. Namun jalan menuju pembentukan badan tersebut menghadapi hambatan, khususnya dengan adanya beberapa kementerian dan lembaga yang berkeras mengajukan diri sebagai koordinator, perilaku reaktif dari pemerintah ini menggambarkan tata kelola yang tumpang tindih di bidang cybersecurity.

Meskipun lemah dalam di bidang legislasi, Indonesia cukup kuat dalam upaya teknis dan prosedural. Kerja sama internasional juga tidak dipandang sebagai masalah, karena Indonesia terus meningkatkan kerja sama internasionalnya dengan berbagai organisasi, ahli keamanan serta forum untuk meningkatkan pemahamannya terhadap ancaman global. Sebagai pengejawantahan prinsip ini di dalam cybersecurity, Indonesia telah menjadi anggota penuh APCERT dan FIRST, serta merupakan salah satu pendiri OIC-CERT.

Terkait upaya teknis, Indonesia secara resmi telah mengakui persyaratan kepatuhan melalui SNI/ISO/EIC 27001:2013 terkait Sistem Manajemen Keamanan Informasi. Untuk meningkatkan kesadaran keamanan dan melacak kemajuan, Indonesia memiliki kerangka untuk menilai keamanan informasi domestik di seluruh lembaga pemerintah. Indeks KAMI (Keamanan Informasi Nasional) misalnya, mengevaluasi lima area keamanan informasi, yaitu tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, dan teknologi. Namun, masih banyak kerja yang harus dilaksanakan.

Tidak adanya peta jalan nasional yang resmi untuk cybersecurity menjadi salah satu agenda mendesak untuk dilaksanakan menurut ITU. Terkait pelaksanaan standar internasional, ITU pada 2015 mencatat bahwa Indonesia belum mengakui secara resmi kerangka cybersecurity (atau sektor spesifik) nasional apapun. Hal serupa juga terjadi pada sertifikasi. Saat ini, Indonesia masih belum memiliki kerangka cybersecurity (dan sektor spesifik) nasional resmi untuk sertifikasi dan akreditasi lembaga nasional dan profesional sektor publik. Saat ini mayoritas standar yang ada di Indonesia merupakan adopsi dari lembaga regional maupun internasional.

Tanpa adanya kemampuan teknis yang cukup untuk mendeteksi dan merespon serangan cyber, negara dan lembaga-lembaganya akan selalu berada di posisi rentan. Seluruh pemangku kepentingan khususnya pemerintah harus mampu mengembangkan strategi dan keterampilan yang diperlukan untuk menangani insiden cyber di tingkat nasional. Strategi dan keterampilan yang dibutuhkan tersebut harus dimasukkan ke dalam kebijakan cybersecurity nasional.

C. **Lanskap Tata Kelola Cybersecurity Indonesia**

Terdapat banyak tantangan dalam mendiskusikan cybesecurity di Indonesia yang dijelaskan pada diagram di bawah ini.

Gambar: Hambatan dan Tantangan Cybersecurity Nasional (sumber: diadaptasi dari Detiknas, 2013)

Hambatan dan tantangan di atas mencakup sejumlah aspek yang harus diatasi agar dapat melaksanakan tata kelola cybersecurity yang efektif. Buku ini mengidentifikasi tiga kesenjangan kunci, yaitu:

1. **Pemahaman dan pendekatan berbeda terhadap cybersecurity**

   Kontroversi seputar tata kelola cybersecurity berawal dari definisinya. Definisi di sini bukan hanya terkait linguistik, namun cara cybersecurity didefinisikan dan dipahami mencerminkan adanya berbagai perspektif dan pendekatan serta kepentingan kebijakan (Kurbalija 2014). Sebagaimana hasil analisis temuan kami, komunitas teknis memandang tata kelola cybersecurity melalui kaca mata teknis dan infrastruktur, serta cenderung berfokus pada pengembangan berbagai standar dan aplikasi. Sebaliknya, organisasi masyarakat sipil khususnya aktivis HAM memandangnya khususnya dari perspektif kebebasan berekspresi dan privasi. Sementara itu penegak hukum dan lembaga intelijen cenderung berfokus pada isu yang terkait dengan perlindungan kepentingan nasional.

   Dengan menyadari bahwa internet bukan hanya sekadar teknologi baru karena internet berperan penting sebagai pendukung pembangunan diperlukan suatu pendekatan baru dalam hal tata kelola internet. Pendekatan baru terhadap teknologi baru ini tidak boleh membatasi diskusi tentang tata kelolanya pada satu perspektif saja. Sebaliknya, tata kelola cybersecurity harus melibatkan berbagai prespektif, baik teknis, hukum, sosial, ekonomi dan pembangunan, serta mendorong semua pemangku kepentingan untuk mengambil bagian. Pendekatan ini juga mencerminkan sifat asli internet, yaitu inklusif sejak lahir, dikembangkan oleh sektor publik dan swasta, akademisi dan masyarakat sipil, serta beroperasi lintas batas negara. Internet secara fundamental selalu bersifat partisipatif dan bottom-up, dan merupakan sebuah ekosistem yang heterogen namun kokoh.

   Di Indonesia, pendekatan partisipatif yang mencerminkan nilai-nilai ini belum terwujud. Meskipun beberapa upaya pelibatan telah dilakukan, pengambilan keputusan masih tetap sepenuhnya di tangan pemerintah dan menghilangkan suara para pemangku kepentingan lain dalam prosesnya. Hal ini juga terjadi pada tata kelola cybersecurity. Meskipun pemerintah sudah menyadari bahwa untuk menjalankan cybersecurity yang efektif diperlukan peraturan, kesadaran dan koordinasi, topik ini masih relatif baru dan belum menjadi prioritas. Ini merupakan tantangan mendasar bagi cybersecurity Indonesia.

2. Kapasitas sumber daya manusia

Kesenjangan digital (digital divide) dan kurangnya sumber daya manusia di area keamanan informasi juga merupakan isu lain yang semakin menambah kompleksitas masalah. Untuk meningkatkan kapasitas SDM di area ini, Kominfo telah mengembangkan kerangka standar kompetensi dalam keamanan informasi dengan bekerja sama dengan sektor swasta dan akademisi. Standar yang dikenal sebagai SKKNI Sektor Keamanan Informasi ini digunakan untuk menetapkan baseline keterampilan teknis bagi mereka yang menjalankan fungsi keamanan informasi di organisasi yang ruang geraknya adalah pelaksanaan keamanan informasi (Kepmenaker No.55/2015). Sejalan dengan standar ini, Direktorat Keamanan Informasi Kominfo secara berkala melakukan program bimbingan teknis dan peningkatan kesadaran untuk mempromosikan penyelenggaraan kursus cybersecurity di perguruan tinggi maupun masyarakat umum, serta memberikan program pelatihan profesional (Kominfo 2015).

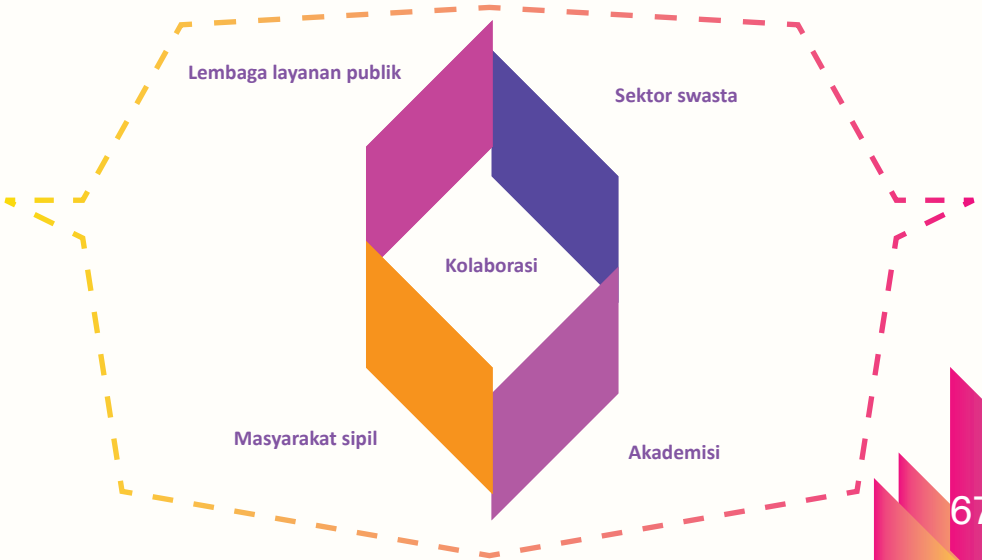
Menurut ITU (2015), Indonesia saat ini memiliki sekitar 500 profesional sektor publik yang bersertifikasi di bawah program sertifikasi yang diakui internasional di cybersecurity seperti ISO270001, CEH, CISA, CISM dan CISSP. Namun jumlah ini belum cukup untuk Indonesia. Sebagaimana dijelaskan oleh seorang perwakilan APJII (wawancara, 2016), SDM di cybersecurity masih didominasi pekerja asing karena masih amat minimnya tenaga ahli lokal.

2. Koordinasi

Masalah yang kompleks memerlukan pendekatan multidimensional. Karenanya, untuk meningkatkan tata kelola cybersecurity, pelaksanaan prinsip multi-pihak (multistakeholderism) menjadi sangat penting. Tanpa adanya kerja sama dan kolaborasi di kalangan pemangku kepentingan (dari lembaga layanan publik hingga sektor swasta, akademisi dan masyarakat sipil), pemecahan masalah isu terkait cybersecurity akan terus menjadi satu dimensi dan tidak lengkap. Diperlukan sebuah mekanisme inklusif yang dapat mengesahkan keputusan sekaligus reflektif dan responsif terhadap kepentingan nasional dan populasi yang terdampak.

Mengingat pentingnya prinsip kejahatan cyber, terdapat kebutuhan mendesak untuk membentuk sebuah lembaga koordinasi (baik dengan menggunakan salah satu unit yang sudah ada maupun dengan membentuk badan baru) yang bertanggung jawab melakukan upaya koordinasi ketika diperlukan, dengan dukungan penuh dari seluruh pihak yang terlibat. Lembaga koordinasi tersebut harus terdiri dari individu-individu yang memiliki integritas dan kompetensi tinggi. Di tingkat operasional, setiap sektor harus memiliki tim tanggap daruratnya sendiri untuk menangani insiden di sektor mereka, dengan peran dan tanggung jawab masing-masing yang jelas.

Tindakan ini harus diarahkan dengan seperangkat peraturan dan peta jalan yang baik tanpa mengabaikan pentingnya membangun kesadaran nasional. Kesimpulannya, trio ‘peraturan, kesadaran dan koordinasi’ harus menjadi mantra yang mendasari tata kelola cybersecurity nasional.



D. Isu Mendasar Tata Kelola Cybersecurity Indonesia

Cybersecurity seringkali disebut sebagai salah satu prasyarat untuk mendorong pertumbuhan e-commerce yang pesat. Tanpa akses internet yang aman dan andal, pelanggan akan enggan memberikan informasi rahasia mereka secara online. Karenanya, tidak mengejutkan ketika sektor bisnis di Indonesia menjadi pemimpin dalam percepatan kemajuan dalam cybersecurity lebih daripada pemerintah sendiri. Namun, sejak munculnya kasus Snowden pada 2013, pemerintah mulai mempertimbangkan taktik mitigasi, antara lain dengan meminta perusahaan-perusahaan internet untuk menyimpan data pribadi masyarakat di sebuah pusat data di wilayah yurisdiksi Indonesia. Kondisi ini juga meningkatkan tensi politik terkait isu tersebut.

Penelitian kami menemukan bahwa fokus cybersecurity di Indonesia adalah pada pertahanan, perang dan kedaulatan. Salah satu fakta yang mendukung klaim ini adalah debat panas terbaru terkait rencana pembentukan Badan Cyber Nasional (BCN). Perspektif BCN terhadap cybersecurity berfokus pada perlindungan infrastruktur kritis seperti bandara publik dan jaringan listrik.

Menteri Kominfo Rudiantara dalam berbagai kesempatan menekankan pentingnya dibentuk sebuah organisasi yang berfungsi melindungi Indonesia dari berbagai ancaman cyber – dari tahap identifikasi hingga proses pemulihan. Meskipun tugas utamanya adalah mencegah serangan cyber, lembaga ini juga akan bertanggung jawab mengembangkan strategi untuk memperkuat pertahanan Indonesia terhadap ancaman dan penyerang cyber. Seiring dengan strategi tersebut, lembaga ini juga akan bekerja meningkatkan kesadaran publik tentang lanskap cybersecurity.

Perkembangan terbaru, pemerintah telah mengeluarkan Peraturan Presiden (Perpres) Nomor: 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), seperti yang tertuang di situs http://setkab.go.id. Dalam Perpres itu disebutkan, disebut BSSN adalah lembaga pemerintah non kementerian, yang berada di bawah dan bertanggung jawab kepada Presiden melalui menteri yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelenggaraan pemerintah di bidang politik, hukum, dan keamanan. Menurut Menkominfo, nantinya badan tersebut akan menyambungkan antara Lembaga Sandi Negara (Lemsaneg) dengan Kementerian Komunikasi dan Informatika. Dibentuknya BSSN ini untuk mempermudah koordinasi yang baik antara lembaga, tidak hanya Lemsaneg dengan Kominfo. Namun masih perlu diamati bagaimana perdebatan seputar hal ini serta publikasi dokumen hukum terkait lembaga ini akan berkembang dalam waktu dekat.

Sejalan dengan ide pembentukan lembaga koordinasi ini, Kominfo juga berencana untuk meluncurkan peta jalan cybersecurity yang bertujuan memberikan Indonesia sebuah acuan (benchmark) cybersecurity nasional untuk sektor non-militer. Menurut Rudiantara, Kominfo beserta beberapa regulator dan operator sektoral spesifik lainnya telah mengembangkan rencana proses bisnis wajib untuk tiga sektor, yaitu keuangan dan perbankan, transportasi, dan energi. Hal tersebut dikemukakan Rudiantara dalam forum diskusi online pada 13 Juli 2016. Dokumen tentang ketiga sektor tersebut akan dapat diakses masyarakat umum pada akhir 2016 (Perwakilan Kominfo, Wawancara, Oktober 2016). Sejalan dengan rencana ini, Kementerian PAN BR akan membantu bisnis menjalani proses tersebut. Meskipun tampak seperti sebuah proses yang solid, namun muncul pertanyaan khususnya terkait lembaga koordinasi yang akan dibentuk. Lembaga seperti apa yang harus bertanggung jawab? Siapa yang harus memimpin? Menteri, Menteri Koordinator, atau pejabat setingkat menteri? Bagaimana mekanisme pelaporannya? Dan seperti apa struktur lembaga ini? Apakah ia akan melapor langsung ke presiden?

Peta jalan ini tampak menjadi bagian dari Perpres yang sedang disusun untuk e-commerce, yang juga akan menjadi bagian dari paket kebijakan ekonomi ke-14. Menurut beberapa laporan media, Perpres ini akan berfokus pada tujuh isu termasuk perpajakan, cybersecurity dan infrastruktur komunikasi. Hal tersebut seperti yang dikatakan pada berita bertajuk "Incentives sought to propel e-commerce" di The Jakarta Post dan "Paket Ekonomi Jilid XIV, Pemerintah Bakal Atur e-Commerce" di Viva.co.id edisi 28 September 2016. Namun pemerintah menolak mengkonfirmasi kapan paket kebijakan baru tersebut akan diluncurkan. Terkait diskursus ini, masyarakat sipil dan komunitas akademik berpendapat bahwa proses pembuatan kebijakan peta jalan dan lembaga koordinasi ini harus menggunakan pendekatan multi-pihak.

Selain isu koordinasi, akan menarik untuk melihat apakah perspektif HAM juga dimasukkan ke dalam proses pembuatan kebijakan ini. Perlindungan HAM (privasi, kebebasan berekspresi, akses internet), dalam hal ini sangat relevan bagi proses pembuatan kebijakan dalam cybersecurity. Hal ini tidak hanya merupakan prioritas berbasis nilai, namun juga merupakan alat praktis untuk menjamin internet tetap terbuka dan aman. Perlindungan akses kepada alat individu sebenarnya secara tidak langsung melindungi data set lembaga atau perusahaan dari pelanggaran yang dilakukan melalui 'pintu belakang' pengguna akhir (end user). Namun kekhawatiran umum pengguna akhir biasanya bukan terkait dengan potensi kerusakan besar (yang seringkali disebabkan ketidaktahuan) akibat pelanggaran, namun lebih terkait privasi dan hak secara umum.

DATA E-KTP INDONESIA BELUM SEPENUHNYA AMAN

Ada isu yang jauh lebih besar ketimbang mempersoalkan lambatnya proses pembuatan eKTP, yaitu masalah keamanan data. Pembuatan e-KTP seri awal melibatkan vendor luar sebagai penyedia solusi sistem manajemen data e-KTP, yaitu PT Biomorf Lone Indonesia. Ketua Indonesia Cyber Security Forum, Ardi Sutedja, melihat persoalan yang lebih besar, yaitu keamanan data e-KTP.

Seluruh informasi tentang warga negara Indonesia, kata dia, seharusnya dilindungi oleh negara. Pernyataan Biomorf bahwa mereka masih menguasai kode sumber sistem e-KTP membuat Ardi khawatir. “Apa jaminannya bahwa kode dan data di dalam sistem belum digandakan oleh pihak ketiga?” kata Ardi. Pengguna saat ini terlalu percaya diri dengan pengetahuan yang dimilikinya tentang keamanan online. Sebagian besar dari mereka tidak melakukan tindakan mendasar dalam hal keamanan online, seperti penggunaan kata sandi yang terlalu sederhana. Yang juga menarik, Ardi menilai proyek e-KTP sejak awal tidak dilengkapi jaminan keamanan data. “Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting,” ungkapnya.

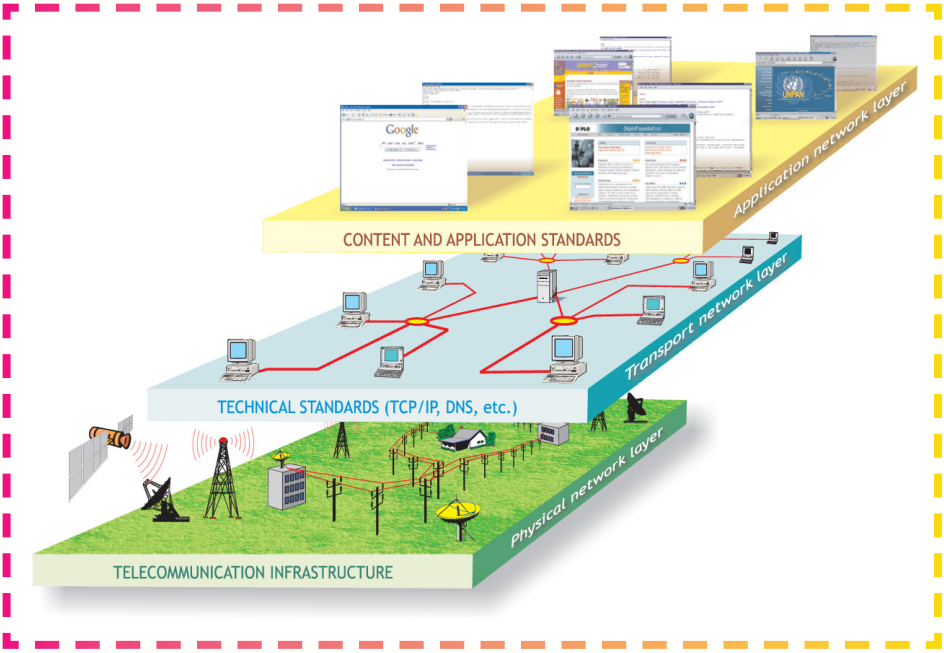
Keamanan siber ini bukan masalah kecil. Tetapi sudah menjadi bagian dari kepentingan nasional”, lanjutnya. Ia pun mengkritisi Badan Cyber Nasional berdasarkan Perpres 53 tahun 2017. “Kalau bicara cyber itu, bukan hanya pertahanan, yang berbau-bau militer. Namanya cyber itu kan luas sekali. Ada kepentingan ekonomi, sosial, budaya, hingga komersial,” paparnya.
(sumber: s.id/8ie, s.id/8if).

BAB IV

Merintis Tata Kelola Cybersecurity Indonesia Berprespektif Multistakeholder

A. Perspektif Multistakeholder

Salah satu cara memahami cara kerja internet adalah dengan membayangkannya sebagai sejumlah lapisan (layer) yang berjenjang sebagaimana digambarkan secara sederhana pada ilustrasi di bawah ini.



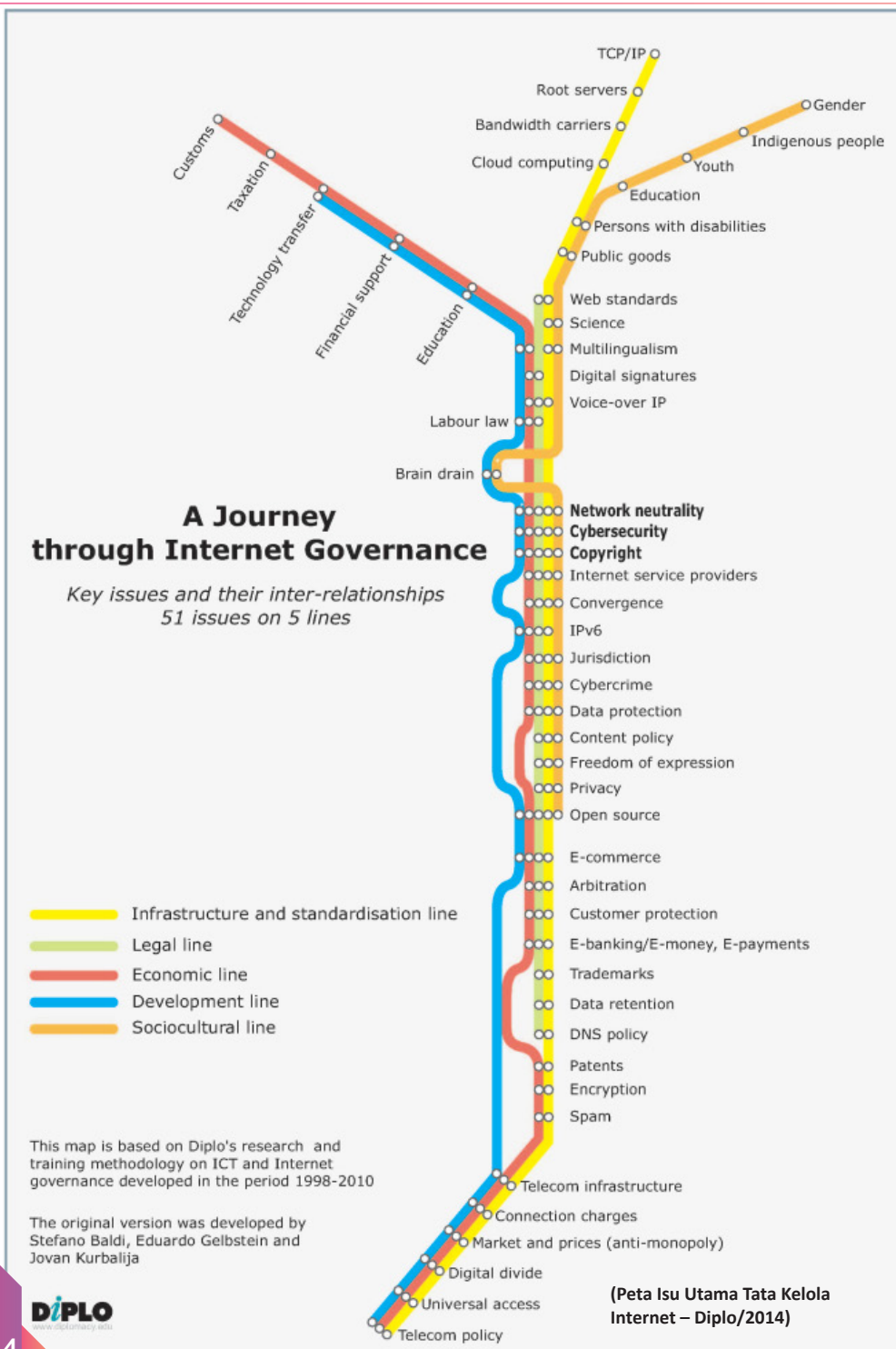
(Ilustrasi Sederhana Lapisan Internet – Diplo/2014)

Lapisan jejaring fisik (physical layer), yang berada di dasar tumpukan, adalah infrastruktur telekomunikasi dan perangkat keras pendukungnya. Lapisan ini memungkinkan setiap perangkat komputer untuk terhubung dan saling berkomumunikasi, sepanjang memang menggunakan standar protocol aturan yang sama. Untuk itulah maka pada lapisan di atasnya, ada lapisan jejaring transport, yang notabene fokus pada penentuan standar teknis protocol seperti TCP/IP, DNS dan sebagainya. Standar teknis tersebut kemudian menentukan bagaimana cara aplikasi dan dan konten dihantarkan dari satu titik ke titik lain dalam jejaring tertentu. Lapisan jejaring aplikasi pada bagian puncak juga menentukan standar aplikasi dan konten yang dapat digunakan dan dinikmati oleh pengguna akhir.

Setiap lapisan ini bekerja secara mandiri. Dengan kemandirian ini, digabung dengan standarisasi ketat dari berbagai protokol yang menjadi ciri khas internet, membuat internet menjadi jejaring yang dapat diperluas dengan pengelolaan yang khas.

Dalam pengelolaan internet, sudah jamak apabila pelaku bisnis telekomunikasi dan internet akan melihat tata kelola internet melalui kacamata pembangunan infrastruktur teknis. Akademisi komputer dan bahasa pemrograman, memberi perhatian kepada pengembangan standar dan aplikasi yang beragam.

Pegiat Hak Asasi Manusia (HAM) dan organisasi masyarakat sipil (civil society organization – CSO) memandang tata kelola internet dari perspektif kebebasan berekspresi, privasi dan hak asasi manusia. Praktisi hukum berkonsentrasi pada yurisdiksi dan penyelesaian sengketa. Adapun pemerintah akan mengambil fokus pada isu-isu yang berkaitan erat pada proses dan perlindungan kepentingan nasional. Sementara itu pelaku bisnis online akan melihat tata kelola internet dari sudut pandang keamanan transaksi online dan menganalisis profil pengguna/pengunjungnya.



(Peta Isu Utama Tata Kelola Internet – Diplo/2014)

Dalam konteks tata kelola internet, setidaknya terdapat 40 hingga 50 isu utama yang relevan dalam diplomasi baik di tingkat nasional, regional, maupun global. Kemudian sejumlah isu utama tersebut diklasifkasikan ke dalam 5 (lima) keranjang aspek, yaitu:

1. Jalur Infrastruktur dan Standardisasi
2. Jalur Hukum
3. Jalur Ekonomi
4. Jalur Pembangunan
5. Jalur Sosial Budaya

Melihat pada peta isu di atas, maka tampak jelas bahwa tidak ada satu pun isu tata kelola internet yang dapat atau boleh dilihat dari satu jalur semata. Sejumlah isu perlu ditinjau, dikaji dan dikelola berdasarkan perspektif dan pendekatan yang komprehensif. Misalnya untuk isu cybersecurity, pendekatan tata kelolanya perlu dilihat dari sudut pandang aspek infrakstruktur dan standarisasi, hukum, ekonomi, pembangunan serta sosial budaya.

B. **Cybercrime Dewasa Ini**

Dewasa ini, setidaknya terdapat empat jenis pelaku kejahatan yang kerap menjadi fokus bahasan dalam diskusi pembuat kebijakan cybercrime secara global:

- Kelompok teroris yang menggunakan internet dari hal yang paling sederhana semisal menggunakan media sosial untuk menyebarkan propaganda radikalisme dan intoleransi, serta menggunakan aplikasi messenger untuk berkomunikasi, hingga hal yang relatif canggih seperti menggunakan layanan anonim online, baik untuk berkomunikasi ataupun meletakkan web mereka, sebagai penunjang proses perencanaan aksi hingga mekanisme perekrutan simpatisan.
- Pelaku pedofil dan jaringan predator online yang menggunakan internet untuk bertukar, menyebarkan, membeli dan menjual gambar eksploitasi atau pelecehan seksual terhadap anak, serta pendekatan seksual (grooming) kepada anak-anak secara online.
- Sindikat kejahatan terorganisir yang memfasilitasi dan/atau memberikan dukungan atas penjualan obat terlarang, senjata gelap, uang dan barang ilegal serta informasi curian.
- Penyerang cyber dan black hacker yang menyasar informasi dan jaringan komputer untuk mendapatkan, menghapus atau mengubah informasi, serta merusak hingga melemahkan keamanan infrastruktur tertentu.

Meskipun definisi cybercrime cukup luas untuk menjangkau kejahatan offline konvensional, kategori yang disebutkan di atas seringkali disebut dalam pembahasan tindakan cybersecurity. Namun, hukum cybercrime umumnya lebih terbatas dalam penerapannya, yaitu pada penyalahgunaan komputer, penipuan, serta pelanggaran melalui komputer (misalnya hanya menyasar penyerang cyber dan black hacker), serta pelanggaran terkait konten.

Sejumlah kebijakan memang perlu disegerakan adanya agar negara dapat berperan optimal dalam mitigasi, investigasi maupun rehabilitasi atas (potensi) ancaman dan kejahatan di ranah online sebagaimana tersebut di atas. Namun upaya-upaya tersebut, tanpa memperhatikan berbagai perspektif kepentingan yang beragam, dapat berimplikasi serius terhadap penegakan hak asasi manusia (HAM).

Contohnya adalah ketika upaya untuk melarang anonimitas di ranah online, termasuk larangan digunakannya layanan enkripsi, seringkali alasannya adalah untuk memerangi kejahatan siber. Namun larangan tersebut sejatinya sangat mungkin menjadi penghambat kebebasan berekspresi dan perlindungan privasi. Tanpa akses kepada layanan anonimitas dan/atau yang terenkripsi, para pegiat HAM dan jurnalis di kawasan konflik, kalangan minoritas maupun kelompok oposisi tidak akan dapat lagi bebas berkomunikasi dan berkumpul di ranah online tanpa rasa takut diintai.

Pelaksanaan sistem pengintaian massal (mass surveillance), yang melanggar esensi hak privasi, rentan menciptakan masyarakat yang tercerabut dari kemampuan berpikir progresif, inovatif dan kreatif. Pemblokiran konten dan/atau penerapan filter internet secara serampangan karena tanpa merujuk pada prosedur yang transparan dan akuntabel, jelas dapat menghambat kebebasan berpendapat di internet

Pemaknaan cybersecurity yang timpang dapat menyebabkan terjadinya sekuritisasi skala besar di internet. Internet lantas dipandang sebagai medan laga, sebuah ranah yang dikuasai para penjahat, pelaku tindak kriminal dan teroris, bukan lagi sebuah ranah untuk edukasi, komunikasi, emansipasi dan berdemokrasi sebagaimana seharusnya.

Dampak yang tidak diharapkan dari implementasi kebijakan cybersecurity terhadap penegakan HAM tidaklah selalu akibat suatu kesengajaan atau telah direncanakan sebelumnya. Namun tentu saja hal ini selalu dapat diprediksi dan dihindari, jika semua pemangku kepentingan semua bersedia menginvestasikan waktu, sumber daya dan pengetahuannya untuk duduk bersama merumuskan kebijakan tersebut. Pendekatan pemangku kepentingan majemuk (multistakeholder) menjadi penting dan signifikan dalam penyusunan kebijakan terkait cybersecurity.

C. **Pemaknaan Multistakeholder**

Faktanya, pendekatan tata kelola internet di suatu negara akan berbeda dengan negara lain. Selalu ada tarik-menarik yang dinamis antara kehendak melakukan kontrol yang ketat oleh negara (baca: pemerintah), dengan kehendak adanya pendekatan yang melibatkan multistakeholder dalam dialog yang partisipatif dan kolaboratif. Memang dalam sistem masyarakat, otoritas dan pengaturan secara umum datangnya dari negara. Namun kewenangan ini dapat dan boleh dialihkan atau dibagi kepada pihak lain.

Jika mengacu pada siapa pihak yang menyusun, mengawasi dan menegakkan aturan ataupun standar, maka akan didapat empat bentuk sistem tata kelola (governance) yang berlaku saat ini. Empat bentuk sistem itu adalah:

- Regulasi tradisional (traditional regulaton),
- Ko-regulasi (co-regulaton),
- Swaregulasi industri (industry self-regulaton),
- Regulasi oleh pemangku kepentingan majemuk (multistakeholder).

Yang dimaksud dengan regulasi tradisional adalah regulasi yang dikembangkan, diundangkan, dan diberlakukan oleh pemerintah di tingkat nasional, baik sendiri ataupun bekerjasama dengan pemerintah lain. Adapun bentuk kedua regulasi yang disebut dengan ko-regulasi adalah pelibatan bersama pemerintah dengan sektor swasta dalam sejumlah proses regulasi, di mana pelaku pasar mendapatkan pendelegasian tugas untuk membangun standar dan menerapkan sanksi atas terhadap sektor publik yang tidak tunduk pada standar (atau aturan) yang telah ditetapkan.

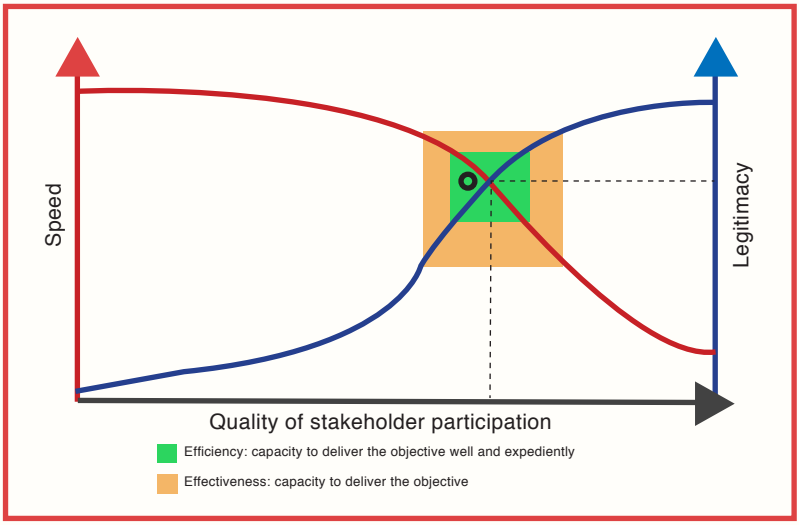
Kemudian bentuk ketiga dari regulasi, yaitu swaregulasi industri, adalah ketika sektor swasta secara mandiri mengembangkan standar teknis dan praktis yang terbaik. Hal ini berlaku umum dalam pengembangan standar dalam inovasi teknis. Hal ini membentuk aksi penegakan kebijakan di mana pelaku industri secara bersama sepakat untuk mengatur dirinya sendiri. Dan tidak sepert pada regulasi tradisional, sistem ini berbasiskan pada standar yang secara sukarela dibangun dan dijalankan.

Adapun variasi sistem tata kelola regulasi yang ke-4, yaitu pemangku kepentingan majemuk (multistakeholder), yang relatif baru. Sistem ini mendorong adanya pelibatan yang dari sejumlah pemangku kepentingan yang beragam untuk menegosiasikan dan membangun kerangka kerja regulasi tertentu. Sistem multistakeholder ini dapat berbentuk sesuatu yang sederhana. Misalnya sebuah kode etik atau perilaku yang disusun oleh organisasi advokasi yang menangani isu tertentu, kemudian disampaikan kepada perusahaan (korporat) atau stakeholder lainnya untuk diadopsi.

Pun multistakeholder ini bisa juga sesuatu yang lebih kompleks, semisal dalam bentuk sebuah upaya besar dari berbagai penjuru dunia untuk mengembangkan dan menyepakati sebuah standar umum berdasarkan kepentingan bersama. Ketahanan dalam kemitraan yang bersifat multistakeholder ini adalah dengan cara:

a). Menghargai kompetensi dan kultur masing-masing mitra (partner)/ pemangku kepentingan (stakeholder),
b). Adanya pendefinisian peran yang transparan dan dapat diandalkan dari setiap stakeholder,
c). Kapabilitas (kemampuan) dari para stakeholder untuk turut serta dalam proses dialog,
d). Keterbukaan di antara sesama stakeholder.

Hal yang tak kalah pentingnya dalam menentukan kelayakan suatu proses multistakeholder, selain legitimasi dan partisipasi sebagaimana telah dijelaskan di atas, adalah tentang efektifitas dan efisiensi proses. Efektifitas adalah tentang kapasitas (sumber daya) yang digunakan untuk mencapai tujuan. Sedangkan efisiensi adalah kemampuan mencapai tujuan dengan cepat dengan hasil yang diharapkan, dengan kapasitas yang ada. Diagram di bawah ini dapat memberikan gambaran tentang keterkaitan sejumlah hal dalam proses multistakeholder.



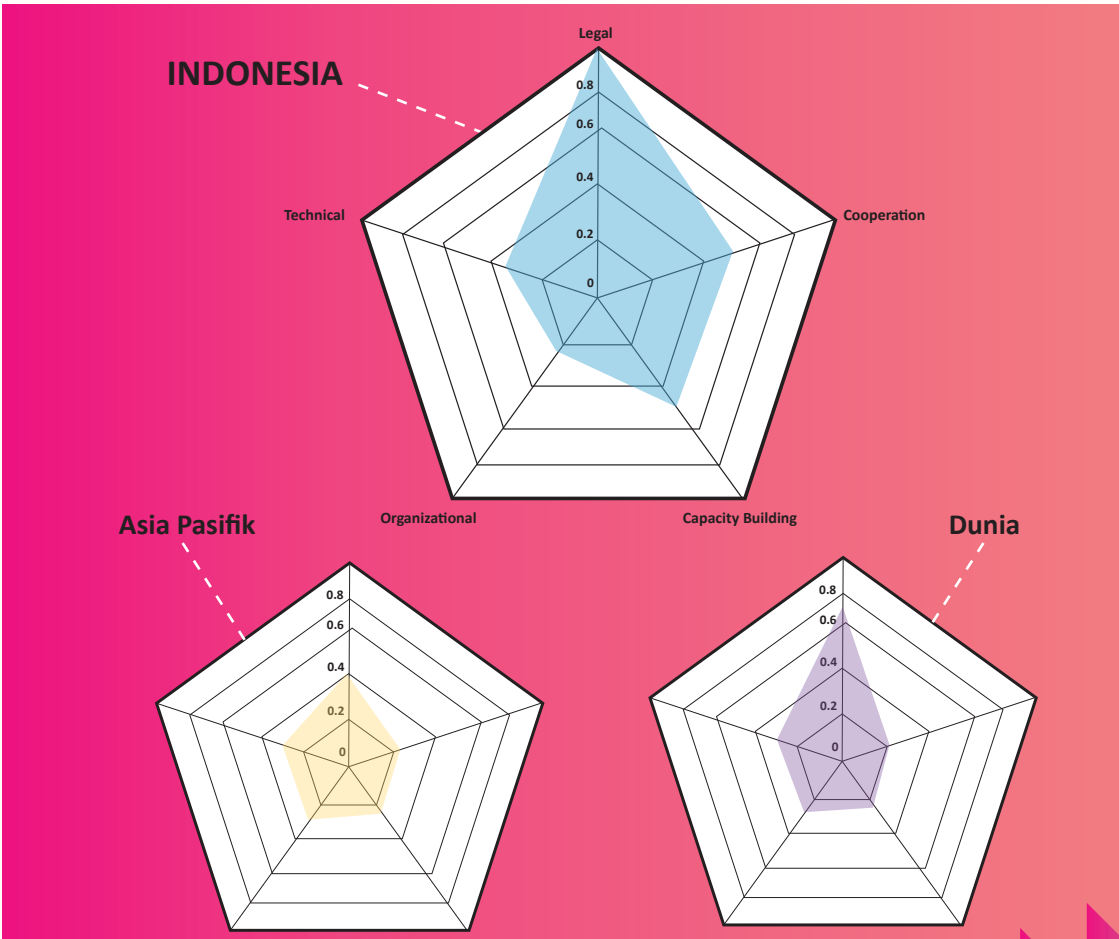
(Proses Multistakeholder – IISD/2004)

Sumbu tegak kiri (merah) mengggambarkan peningkatan kecepatan proses (speed). Kualitas partisipasi sangat tergantung pada jumlah, kualitas, dan keberagaman mereka yang berpartisipasi. Semakin berkualitas stakeholder yang terlibat (titik pada panah hitam horizontal semakin ke kanan), maka proses mengambil keputusan akan semakin membutuhkan waktu. Adapun sumbu tegak kanan (biru) merupakan tingkat legitimasi (legitimacy). Semakin berkualitas stakeholder yang terlibat, maka proses mengambil keputusan akan semakin absah (legitimate).

Persimpangan atau titik potong dua kurva di atas (poin "O"), antara kurva merah (kecepatan) dan kurva biru (legitimasi), disebut sebagai titik "efisiensi optimal". Kotak hijau persegi disekitar titik potong tersebut dapat dianggap sebagai "zona efisiensi". Adapun kotak coklat persegi yang lebih besar, disebut sebagai "zona efektifitas", menunjukkan bahwa proses tetap efektif, tetapi tidak efisien. Di luar kedua kotak ini, dapat dikatakan bahwa proses berjalan tidak efektif dan tidak efisien.

D. Posisi Indonesia

Presiden Indonesia, Joko "Jokowi" Widodo, pada akhir September 2016 mengatakan bahwa Indonesia mengalami peningkatan kejahatan siber yang drastis, dengan jumlah kasus yang tumbuh menjadi 389 persen pada tahun 2014 hingga 2015. Jokowi juga menginformasikan bahwa sebagian besar kasus terjadi di sektor berbasis e-commerce dan pada tahun 2013 Indonesia telah menjadi target terbesar kedua kejahatan siber di seluruh dunia. Kebutuhan terhadap keamanan siber telah menjadi tantangan baru dalam hal kesiapan lembaga pemerintah Indonesia.



(Representasi grafis dihasilkan dari informasi yang dikumpulkan untuk GCI 2014, data direpresentasikan dalam grafik radar dengan masing-masing menunjukkan skor GCI dari lima kategori – ITU/2014)

Rank	Country	Index
1	Singapore	0.925
2	USA	0.919
3	Malaysia	0.893
4	Oman	0.871
5	Estonia	0.846
6	Mauritius	0.83
7	Australia	0.824
8	Georgia	0.819
9	France	0.819
10	Canada	0.818
11	Russia	0.788
12	Japan	0.786
13	Norway	0.786
14	UK and Northern Ireland	0.783
15	Republic of Korea	0.782
16	Egypt	0.772
17	Netherlands	0.76
18	Finland	0.741
19	Sweden	0.733
20	Switzerland	0.727

Rank	Country	Index
21	Spain	0.718
22	New Zealand	0.718
23	Israel	0.691
24	Latvia	0.688
25	Thailand	0.684
26	India	0.683
27	Germany	0.679
28	Qatar	0.676
29	Ireland	0.675
30	Belgium	0.671
31	Mexico	0.66
32	Uruguay	0.647
33	Austria	0.639
34	Italy	0.626
35	China	0.624
16	Poland	0.622
37	Denmark	0.617
38	Czech Republic	0.609
39	Rwanda	0.602
40	Luxembourg	0.602

Rank	Country	Index
41	Philippines	0.594
42	Brazil	0.593
43	Belarus	0.592
44	Tunisia	0.591
45	Croatia	0.59
46	Romania	0.585
47	Turkey	0.581
48	Bulgaria	0.579
49	Kenya	0.574
50	Colombia	0.569
51	Saudi Arabia	0.569
52	Nigeria	0.569
53	UEA	0.566
54	Azerbaijan	0.559
55	Morocco	0.541
56	Uganda	0.536
57	Hungary	0.534
58	Republic of Korea	0.532
59	Brunei Darussalam	0.524

Rank	Country	Index
61	Macedonia	0.517
62	Portugal	0.508
63	Lithuania	0.504
64	South Africa	0.502
65	Ukraine	0.501
66	Iran	0.494
67	Cyprus	0.487
68	Panama	0.485
69	Argentina	0.482
70	Greece	0.475
71	Bahrain	0.467
72	Ecuador	0.466
73	Pakistan	0.447
74	Algeria	0.432
75	Botswana	0.43
76	Indonesia	0.424
77	Montenegro	0.422
78	Sri Lanka	0.419
79	Moldova	0.418
80	Cote d'Ivoire	0.416

Menurut Global Cybersecurity Index (GCI) atau Index Keamanan Siber Global 2014 yang dirilis oleh International Telecommunication Union (ITU), Indonesia menduduki peringkat nomor 5 dalam kesiapan terhadap keamanan siber di antara negara-negara Asia Pasifk (atau nomor 13 di antara 105 negara diseluruh dunia).

Tingkat masing-masing pembangunan negara dianalisis dalam 5 (lima) kategori: Tindakan Hukum, Tindakan Teknis, Tindakan Organisasi, Pengembangan Kapasitas dan Kerja sama. Indeks bertujuan melihat kesiapan keamanan siber negara, bukan indikator kerentanan secara khusus.

Adapun berdasarkan Asia-Pasifik Cybersecurity Dashboard 2015 yang dirilis oleh Business Software Alliance (BSA), Indonesia berada di tahap awal pengembangan strategi keamanan siber nasional. Secara global, kerangka keamanan siber hukum harus diperkuat dan harus dibangun di atas prinsip-prinsip utama, antara lain: kepercayaan dan kerjasama pengampu kepentingan (stakeholder), menghormati privasi dan kebebasan sipil, serta edukasi dan advokasi mengenai keamanan siber.

Untuk mencapai tujuan di atas, khususnya terkait "kepercayaan dan kerjasama kemitraan antar pengampu kepentingan", maka ada beberapa hal pokok yang harus diperhatikan terkait dengan kontribusi sumber daya para stakeholder yang berpartisipasi. Misalnya, sumber daya yang dikontribusikan oleh stakeholder kepada proses kemitraan stakeholder, haruslah serelevan mungkin dengan inti kompetensi dan program kerja masing-masing. Kontribusi tersebut lantas perlu diletakkan dalam visi-misi dan tujuan bersama, dengan pembagian peran dan tanggung-jawab yang ajeg terhadap masing-masing stakeholder. Hal ini akan menjadi salah satu pendorong atau kontribusi terhadap perwujudan proses yang berkelanjutan.

Demikianlah, melalui tulisan ini secara bersama kita akan dapat memahami dinamika dan problematika tata kelola internet pada umumnya, melalui sebuah pendekatan multistakeholer secara inklusif, kolaboratif dan partisipatif. Tulisan ini juga diharapkan dapat membantu memetakan semangat dan implementasi multistakeholder Indonesia untuk mewujudkan tata kelola cybersecurity yang selaras dengan penegakkan HAM.

Sumber literatur rujukan (urut abjad):

Asia-Pacific Cybersecurity Dashboard 2015 (BSA, 2015)
http://cybersecurity.bsa.org/2015/apac/

Cybersecurity Policy for Human Rights Defenders (Global Partners Digital, 2016)
https://www.gp-digital.org/publication/travel-guide-to-the-digital-world-cybersecurity-policy-for-human-rights-defenders/

Global Cybersecurity Index & Cyberwelness Profiles (ITU, 2014)
http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Governance and Multi-stakeholder Processes (IISD, 2004)
http://portals.wi.wur.nl/files/docs/msp/sci_governance1.pdf

Internet Governance: The Role of Multistakeholder Organizations (Univ. of Colorado, 2012)
http://siliconflatirons.org/documents/publications/report/InternetGovernanceRoleofMSHOrgs.pdf

Introduction to Internet Governance, 6th Ed. (Diplo Foundation, 2014)
https://www.diplomacy.edu/resources/books/introduction-internet-governance

Multistakeholder Dalam Pengaturan Internet: Apa dan Mengapa? (ELSAM, 2014)
http://perpustakaan.elsam.or.id/index.php?p=show_detail&id=14247

Multistakeholder Partnership (Global Knowledge Partnership, 2003)
https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/2117.pdf

Multi-Stakeholder Partnerships in ICTs for Development (APC, 2007)
https://www.apc.org/en/system/files/catia_ms_guide_EN-1.pdf

New Forms of Governance: Social Regulations of the Global Market (Univ. of Marryland, 2003)
http://web2.law.buffalo.edu/faculty/meidinger/823/Haufler.pdf

You Only Click Twice: FinFisher's Global Proliferation (Citizen Lab, Univ. of Toronto, 2013)
https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

https://www.rappler.com/indonesia/data-dan-fakta/192885-badan-siber-sandi-negara-bssn

http://www.digianalysys.com/itu-global-cyber-security-index-2017/

http://komite.id/2018/01/10/bssn-next-gen-cyber-security-institution/