PUBLISHED IN THE ARY SUTA CENTER SERIES ON STRATEGIC MANAGEMENT JANUARY 2019

Belajarlah Sampai Ke Finlandia

Strategi Keamanan Siber yang Menyeluruh dan Perubahan Budaya

Oleh Reza A.A Wattimena
Sekolah Kajian Stratejik dan Global
Pascasarjana Universitas Indonesia

Abstrak

Tulisan ini merupakan kajian terhadap strategi sistem keamanan siber menyeluruh yang dikembangkan Finlandia. Metode yang digunakan adalah analisis kebijakan resmi strategi siber Finlandia, beserta upaya menarik butir-butir pembelajaran untuk kepentingan Indonesia dalam bentuk perubahan budaya. Tulisan ini mengacu pada kerangka berpikir yang dikembangkan oleh Aapo Cederberg, seorang penasihat eksekutif di F*innish Information Security Cluster* di Finlandia, sekaligus *CEO* dari *Cyberwatch Finland*. Strategi sistem keamanan siber Finlandia akan dijelaskan dengan menyeluruh, sekaligus pengembangan budaya sigap, presisi, koordinasi dan prioritas kelembagaan yang kiranya amat penting untuk konteks Indonesia.

Kata-kata Kunci: Sistem Siber, Strategi Keamanan Siber, Keamanan Siber, Perubahan Budaya, Logika Asimetri

Pepatah kuno menyatakan, belajarlah sampai negeri Cina. Memang, pemikiran Cina banyak mengandung kebijaksanaan tinggi yang baik untuk kehidupan. Namun, di abad 21 ini, sumber kebijaksanaan ternyata tidak hanya ditemukan di negeri Cina, tetapi juga di Finlandia. Ia terkenal bukan hanya sebagai negara dengan mutu pendidikan terbaik di dunia,[1] tetapi juga sebagai salah satu negara dengan strategi keamanan siber (*cybersecurity strategy*) terbaik di dunia.[2]

Dewasa ini, keamanan siber adalah persoalan yang amat penting dan kompleks untuk ditanggapi. Hampir semua negara menggunakan sistem siber untuk mengolah informasi terkait dengan kependudukan, politik, ekonomi sampai dengan keamanan. Sistem siber ini merupakan sistem trandisipliner yang meliputi berbagai bidang keilmuan, dari hukum, hubungan internasional sampai dengan teknologi informasi dan komunikasi. Maka dari itu diperlukan sebuah strategi menyeluruh keamanan siber yang meliputi juga perubahan budaya.

Tulisan ini hendak membahas strategi keamanan siber dan perubahan budaya dengan mempelajari sistem yang sudah ada di Finlandia. Bagian pertama tulisan ini hendak membahas sistem keamanan siber menyeluruh Finlandia. Bagian kedua menarik beberapa pelajaran dalam bentuk perubahan budaya untuk Indonesia. Bagian ketiga merupakan kesimpulan dari keseluruhan tulisan ini. Acuan utama tulisan ini adalah karya Aapo Cederberg, Stefanie Frey[3] dan beberapa penelitian yang telah dilakukan sebelumnya oleh penulis (Reza A.A Wattimena).

1.Sistem Keamanan Siber Menyeluruh di Finlandia

Revolusi industri yang keempat mendorong orang untuk masuk dan menghuni dunia siber dengan amat cepat dan intensif. Hal yang sama terjadi di tingkat negara, maupun di komunitas internasional. Pengolahan data dalam jumlah besar, seperti data kependudukan dan data finansial, kini sepenuhnya menggunakan komputer.[4] Persoalan utamanya lalu adalah, bagaimana mempersiapkan masyarakat secara luas, supaya bisa menggunakan dunia siber dengan efisien sekaligus aman? Atau,

[1] Lihat (Wattimena, Rumah Filsafat, 2016) Belajarlah sampai ke Skandinavia
[2] Lihat (Cederberg, 2018)
[3] Lihat (Frey, 2018)
[4] Lihat (Frey, 2018)

dirumuskan secara lebih sederhana, bagaimana meningkatkan kesadaran siber masyarakat secara luas?

Di masyarakat berteknologi tinggi, informasi dan pengetahuan adalah sumber kekuatan.[5] Sebaliknya, pihak-pihak yang tak mampu mendapatkan dan mengelola informasi serta pengetahuan akan ketinggalan kereta, dan kalah dari persaingan global. Ini juga ditambah dengan bahaya yang muncul, akibat dari serangan-serangan siber yang terjadi. Tanpa strategi yang bersifat menyeluruh dalam soal keamanan siber, sebuah masyarakat akan terus menjadi korban serangan siber, dan mengalami kerugian besar di berbagai bidang.

Sebuah negara bisa memiliki kekuatan militer yang besar, namun tetap rentan di hadapan berbagai bentuk serangan siber. Memang, persoalan keamanan siber lebih luas dari sekedar pendekatan keamanan lama yang hanya berpijak pada angkatan bersenjata dan polisi semata. Dalam konteks keamanan siber, seluruh unsur masyarakat harus terlibat di dalam proses perumusan dan penerapan strategi keamanan siber. Tentu saja, kepemimpinan politik tetap memegang peranan terpenting dalam hal ini.

Persoalan keamanan siber bukanlah hanya persoalan politik dan keamanan satu negara semata. Kehadiran dan perkembangan dunia siber sebagai sistem pengolahan informasi dan komunikasi secara massal tidak hanya menguntungkan banyak negara, tetapi juga menjadi resiko keamanan yang besar. Para pengguna komputer yang aktif di dunia siber, namun buta terhadap persoalan keamanan siber, akan mudah sekali menjadi korban dari serangan siber. Di mata para teroris siber, celah kecil di dalam sistem siber akan menjadi peluang untuk menciptakan kerusakan besar.

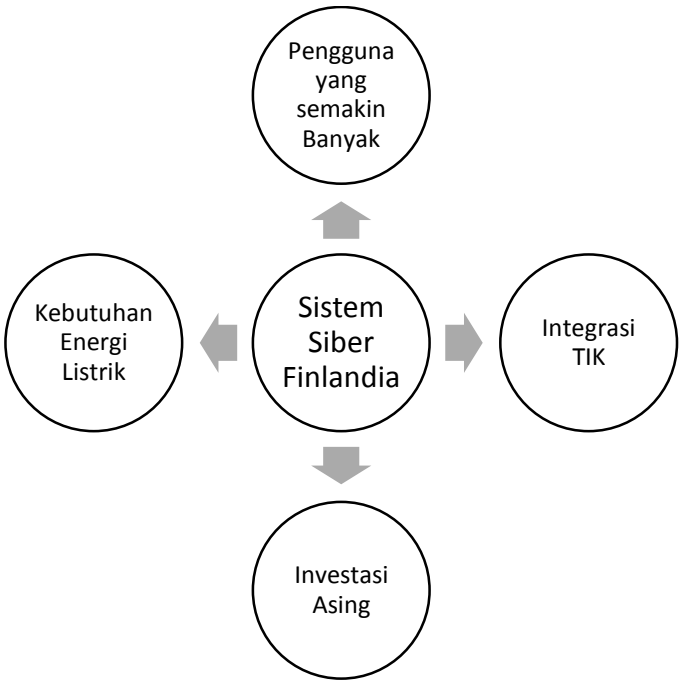
Adalah tugas utama negara untuk melindungi rakyatnya dari berbagai ancaman. Pemerintah Finlandia secara khusus memegang teguh prinsip ini. Prinsip ini diterjemahkan secara nyata melalui pengolahan data informasi dan komunikasi yang, sayangnya, amat rentan terhadap berbagai bentuk serangan siber. Ada beberapa unsur kunci di dalam sistem siber Finlandia, yakni intensitas penggunaan teknologi informasi yang semakin meningkat, semakin besarnya investasi asing,

[5] Bdk (Charles J . Brooks, 2018)

integrasi tak terpisahkan antara teknologi informasi dan komunikasi dan penggunaan energi listrik yang amat besar untuk menopang sistem siber yang ada.[6]

Gambar 1.[7]

Latar Belakang Sistem Siber Finlandia



Di Finlandia, strategi keamanan siber berjalan searah dengan Strategi Keamanan Nasional. Dalam hal ini, pemerintah adalah pihak yang paling bertanggung jawab di dalam soal keamanan dengan berbagai kementrian dan institusi yang memiliki tugasnya masing-masing. Khusus dalam soal keamanan siber, pemerintah membentuk *Cyber Security Center* untuk menangani berbagai persoalan terkait dengan keamanan siber. Dalam soal ini, ukuran keberhasilan sebuah institusi siber adalah keberhasilannya melakukan pencegahan dan penangkalan terhadap berbagai bentuk serangan yang terjadi (*pre-emptive measures*).

[6] Kerangka umum mengacu pada (Cederberg, 2018)
[7] Hasil rumusan penulis

Strategi Siber Finlandia selalu dalam keadaan siap, baik dalam keadaan normal maupun pada masa-masa darurat. Ini terjadi, karena semua organisasi yang bertanggung jawab soal keamanan siber memiliki rencana yang bersifat menyeluruh. Ini setidaknya terwujud dalam banyaknya rencana kontingensi, ketika prosedur standar gagal menangani serangan siber yang mungkin terjadi. Kesadaran siber semacam ini berkembang tidak hanya di lembaga pemerintah, tetapi juga di dunia bisnis.

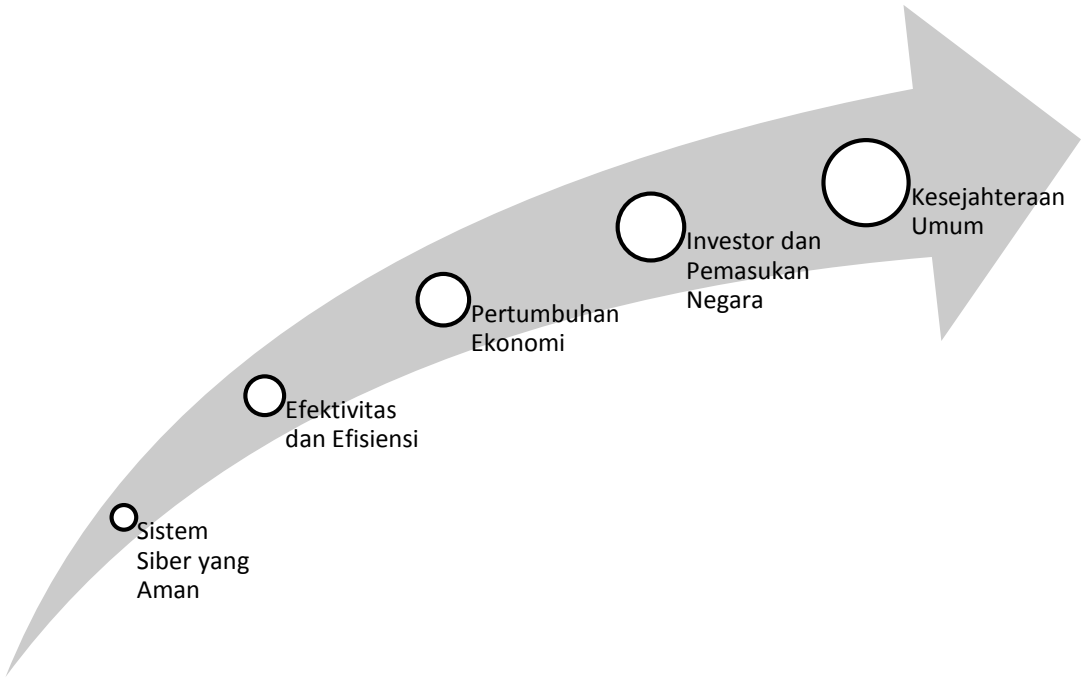
Mengapa keamanan siber dianggap begitu penting di Finlandia? Logika penjelasan yang ditawarkan amatlah penting dan menarik untuk dipahami. Ruang siber yang aman akan membuat semua pengelolaan informasi menjadi efisien. Ini memudahkan semua orang untuk bekerja di berbagai bidang kehidupan, yang nantinya berujung pada peningkatan pertumbuhan ekonomi.

Dengan ekonomi yang maju, dan sistem siber yang aman, Finlandia akan menarik perhatian investor dari luar negeri. Ini juga akan menambah jumlah lapangan kerja baru, serta pemasukan negara dalam bentuk pajak. Ini lalu digunakan untuk menyokong kebutuhan negara lainnya, terutama untuk mempertahankan tradisi negara kesejahteraan (*welfare state*) yang menekankan keseimbangan antara kesejahteraan ekonomi di satu sisi, dan kelestarian lingkungan di sisi lain.[8] Dalam hal ini dapatlah dilihat keterkaitan mendalam antara sistem siber yang aman dengan perkembangan masyarakat secara keseluruhan.

[8] Lihat (Reza A.A Wattimena, Narrowing the Global Gap: Eco-Social Market Economy as New Perspective to Deal with Global Economic Inequality and Economic Insecurity in 21st Century, 2017)

Gambar 2[9]

Sistem Siber dan Kesejahteraan Umum di Finlandia



Dari tahun ke tahun, jumlah serangan siber di seluruh dunia terus meningkat. Motifnya beragam, mulai dari motif ideologis, finansial, industrial dan bahkan politik yang dilakukan oleh negara. Pelaku serangan siber ini disebut juga sebagai teroris siber. Dampak serangan siber sangatlah merusak, mulai dari pencurian data pribadi, data finansial sampai dengan pencurian kode nuklir yang bisa menghancurkan sebuah negara. Ini seringkali ditutupi dari media massa, guna mencegah panik di masyarakat luas. Dalam konteks perang antar negara, serangan siber seringkali dipadukan dengan serangan militer yang lebih bersifat tradisional.[10]

Dunia siber memang mengatur banyak unsur di dalam hidup bersama, mulai dari keamanan, pelayanan publik, data finansial bisnis sampai dengan data operasional industri. Di satu sisi, semua bentuk komunikasi dan pengolahan informasi menjadi begitu cepat dan efektif. Di sisi lain, resiko pencurian data, dan bahaya yang mengikutinya, juga semakin besar. Ketika sistem siber rusak, karena serangan teroris

[9] Rumusan dari penulis
[10] Lihat (Wattimena, Bisakah Perang Dihindari?, 2018)

atau negara lain, maka banyak bidang kehidupan juga akan ikut lumpuh, mulai dari pengolahan data kependudukan, data finansial, data industrial sampai dengan pelayanan publik yang menunjang kehidupan banyak orang.

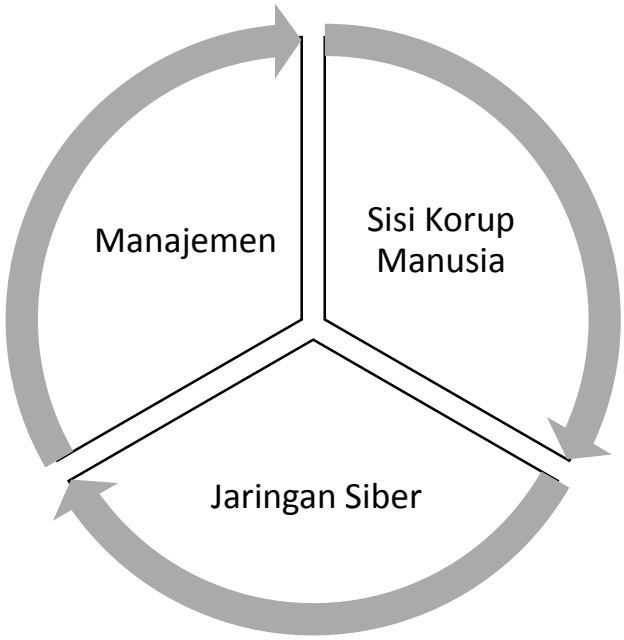
Serangan siber, walaupun kerap kali dirahasiakan dampaknya, memiliki akibat yang amat merusak. Biasanya, serangan tersebut menuntut pemerintah atau organisasi tertentu untuk memberikan uang, atau data tertentu yang sifatnya rahasia. Beberapa negara bahkan memandang serangan siber sebagai sebuah deklarasi perang, terutama jika berhasil dibuktikan, bahwa serangan tersebut dilakukan oleh negara tertentu. Jika dilakukan oleh organisasi non-negara, maka pelakunya digolongkan sebagai teroris yang menjadi musuh negara.

Dalam konteks serangan siber, kelompok kecil teroris, atau negara dengan kekuatan militer yang lemah, bisa melakukan serangan dengan dampak yang amat merusak terhadap negara lainnya. Dalam arti ini, serangan siber membongkar pengertian lama tentang arti dari kekuatan militer sebuah negara, atau sebuah kelompok. Finlandia, sebagai negara yang banyak bergantung pada sistem siber untuk mengolah informasi dan pola komunikasinya, sudah seringkali mengalami serangan siber terhadap jaringan sibernya. Motifnya beragam, mulai dari pencurian informasi sampai dengan manipulasi data untuk kepentingan kelompok teroris tertentu.

Korbannya pun bukan hanya institusi pemerintah Finlandia saja, tetapi juga milik swasta. Kelemahan sistem siber ditemukan, dan kemudian dimanfaatkan oleh para teroris siber. Serangan siber pun kerap kali direncanakan secara matang, baik dalam soal waktu maupun metode serangan, terutama soal penciptaan dan pengembangan malware sebagai metode serangan siber yang paling banyak digunakan. Yang juga membuat keadaan semakin sulit, serangan siber bisa dilakukan dari tempat manapun di dunia, sejauh ia terhubung ke jaringan internet.

Gambar 3.

Tiga Titik Serang di Dunia Siber Finlandia



Serangan siber memanfaatkan kelemanan sistem siber Finlandia di tiga titik. Yang pertama adalah titik kelemahan manusiawi sebagai penjaga sistem siber, terutama dengan memanfaatkan sisi korup dari manusia itu sendiri.[11] Yang kedua adalah dengan memanfaatkan kelemahan organisasi yang ada, termasuk di dalamnya celah tata kelola yang bisa digunakan untuk melancarkan serangan siber. Yang ketiga, tentu saja, adalah kelemahan sistem jaringan komputer itu sendiri. Sistem jaringan komputer perlu untuk terus disesuaikan dengan perkembangan terbaru, supaya tetap terjamin keamanannya.

Harus diakui, kehadiran sistem siber mengubah banyak hal, mulai dari tata politik dan ekonomi global, sampai dengan kehidupan pribadi setiap orang. Di dalam dunia nyata, yakni dunia non siber, ruang dan waktu berlaku mutlak. Namun, perkembangan teknologi informasi dan komunikasi, yang melahirkan dunia siber,

[11] Bdk (Wattimena, Filsafat Anti Korupsi, 2012)

membengkokkan ruang dan waktu tersebut, sekaligus mengubah hukum-hukum yang ada di dalamnya. Proses pengolahan informasi dan komunikasi menjadi begitu cepat, sekaligus penuh dengan resiko.

Dalam arti ini, dapat juga dikatakan, bahwa dunia siber adalah dunia baru yang berbeda dengan dunia fisik, walaupun keberadaannya tak bisa dilepaskan dari dunia fisik. Server dan sistem operasi masih berada di dunia fisik. Persimpangan antara dunia fisik dan dunia siber ini jelas menuntut cara berpikir baru, baik di dalam penggunaan maupun di dalam pengamanannya. Pengaruhnya terhadap perubahan tata politik global pun tak bisa diremehkan.

Kehadiran dunia siber menciptakan asimetri di dalam politik global. Logikanya begini. Di masa lalu, kekuatan militer sebuah negara tergantung pada dua hal, yakni sumber daya yang ada, dan pasukan yang besar, baik di darat, laut maupun udara. Dengan kekuatan militer yang besar, sebuah negara bisa memenuhi kepentingannya di panggung politik global. Namun, dengan perkembangan sistem siber, hal ini tidak lagi sepenuhnya benar.

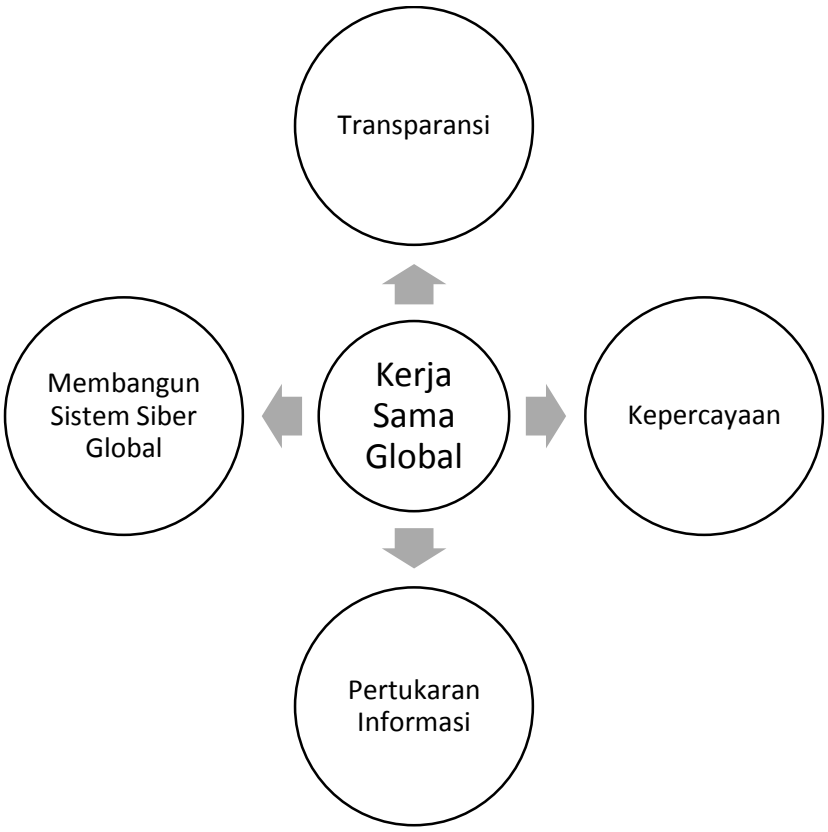
Keberadaan satu orang, yang menguasai sistem siber dengan baik, bisa menjadi senjata yang amat membahayakan bagi suatu negara, walaupun negara itu memiliki sumber daya militer yang kecil. Kekuatan siber tidak bergantung pada sumber daya militer, tetapi pada kehadiran orang-orang yang menguasai *programming* sistem siber, dan mampu menerapkannya sesuai keperluan. Dengan kekuatan siber yang besar, sebuah negara bisa memiliki pengaruh besar di dalam politik global. Inilah yang disebut logika asimetri di dalam politik global.

Kekuatan siber (*cyber power*) mengubah seluruh pemahaman tentang keamanan, baik keamanan militer maupun keamanan sipil. Batas-batas negara pun menjadi relatif di bawah hantaman kehadiran sistem siber di berbagai negara. Di abad 21 ini, ini tidak dapat dihindari, karena hampir semua negara sudah menggunakan dunia siber untuk menyimpan data, maupun mengolah informasi yang mereka punya. Upaya mengatur tata kelola dunia siber jelas tidak bisa dilakukan oleh satu atau beberapa negara semata. Kerja sama global harus menjadi prioritas utama.[12]

[12] Bdk, (Harari, 2018)

Gambar 4.[13]

Kerja Sama Global dalam Keamanan Siber



Beberapa contoh kerja sama internasional yang diikuti pemerintah Finlandia terkait dengan sistem siber yang ada adalah soal hak kekayaan intelektual, paten, standar telekomunikasi internasional serta hukum dan norma internasional di dunia siber.[14] Semua bentuk kerja sama dibangun atas dasar kepercayaan, walaupun lingkupnya memang belum seluas dunia itu sendiri. Kerja sama ini penting, karena menyentuh empat tujuan besar, yakni meningkatkan transparansi dan kepercayaan antar negara, meningkatkan kemampuan untuk saling bertukar informasi serta membangun sistem siber global yang aman dari berbagai bentuk serangan.

[13] Hasil rumusan penulis
[14] Bdk (Hansel, 2013)

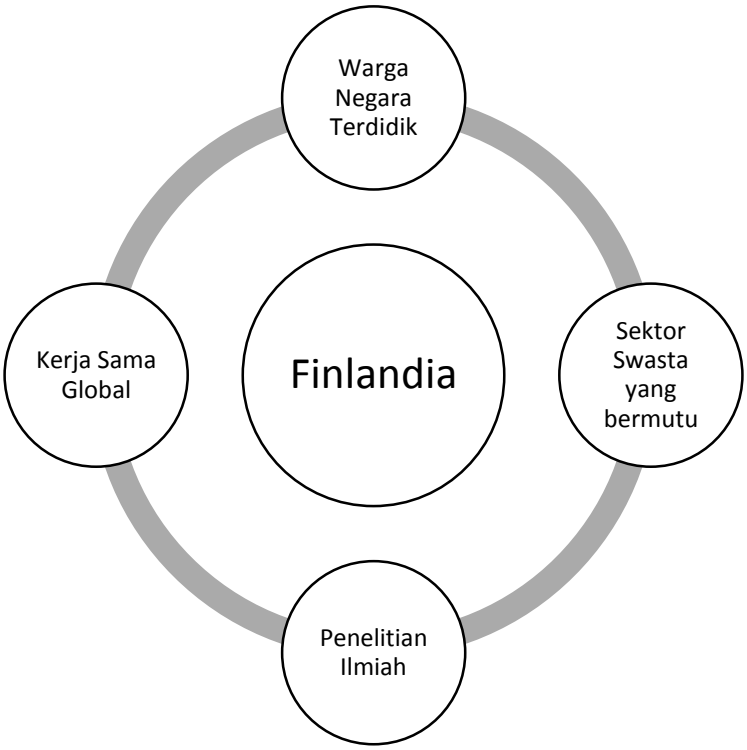
Kerja sama internasional ini juga penting di dalam menopang sistem finansial global. Sistem finansial ini menjadi jangkar bagi proses pembangunan di berbagai negara, terutama negara-negara berkembang. Maka dari itu, sistem finansial global, yang amat bergantung pada keberlangsungan sistem siber yang ada, perlu untuk terus dijaga keamanannya dari berbagai serangan. Pemerintah Finlandia sudah lama menyadari ini, dan bergerak lebih jauh dengan menerapkan kerja sama pemerintah dan swasta untuk memberi penghukuman yang selayaknya bagi para pelaku serangan siber.

Dalam hal ini, tanggung jawab terbesar ada di tangan pemerintah. Tugas utama pemerintah Finlandia, dalam soal keamanan siber, adalah merumuskan panduan politik dan strategis untuk keamanan siber. Pemerintah juga wajib membuat berbagai keputusan tentang sumber daya negara yang digunakan untuk memperketat pengamanan siber yang ada. Di Finlandia, setiap kementerian dan lembaga negara bertanggung jawab untuk keamanan siber yang berada di dalam ranah otoritasnya.

Paradigma yang digunakan pemerintah Finlandia adalah paradigma kesiapan total. Ini melingkupi pemerintah sebagai penanggung jawab utama, semua institusi dan masyarakat sebagai keseluruhan. Inilah yang disebut sebagai paradigma keamanan siber yang menyeluruh. Paradigma ini juga ditopang oleh empat hal. Yang pertama adalah warga negara yang terdidik. Pendidikan yang bermutu menjadi kunci dari ketahanan nasional, tidak hanya dalam konteks dunia siber, tetapi keamanan secara keseluruhan.

Gambar 5.[15]

Fondasi Strategi Menyeluruh Keamanan Siber Finlandia



Yang kedua adalah perusahaan-perusahaan swasta dengan manajemen profesional dan pasar global. Pemerintah mendukung berkembangnya perusahaan-perusahaan ini dengan menyediakan aturan serta birokrasi yang bersih dan efisien. Yang ketiga adalah penelitian ilmiah dan pengembangan yang berkelanjutan dari berbagai universitas dan institusi penelitian yang ada. Pemerintah juga berperan besar dalam menyediakan pendidikan dan penelitian yang bermutu bagi rakyatnya.

Yang keempat adalah kerja sama internasional dengan berbagai negara maupun institusi untuk pengembangan bersama. Dari keempat hal ini, Finlandia kemudian mengembangkan *Finnish Cyber Security Strategy* dengan ukuran dan

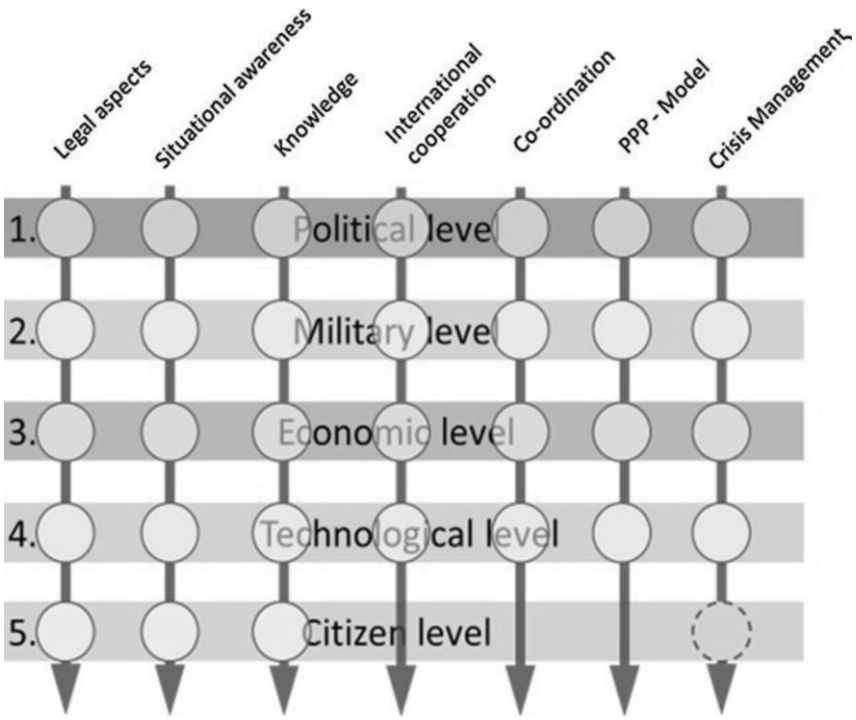
[15] Rumusan Penulis

tujuan yang jelas. Strategi ini digunakan untuk menanggapi semua bentuk serangan siber. Ia juga digunakan untuk menjamin, bahwa sistem siber berjalan lancar di dalam menopang tata politik dan ekonomi Finlandia.

Strategi keamanan Siber menyentuh unsur jangka panjang, yakni menjadikan Finlandia sebagai negara teraman dalam soal strategi siber, sekaligus juga jangka pendek, yakni kerja sama yang efektif dan efisien di dalam mencegah sekaligus menanggulangi berbagai bentuk serangan siber yang mungkin terjadi. Ini menjadi amat penting, karena di abad 21, serangan teroris berlangsung di dua tingkat, yakni serangan fisik dan serangan siber sekaligus. Kedua bentuk serangan ini saling menopang untuk mewujudkan tujuan dari serangan teroris tersebut, yakni menyebarkan teror kepada masyarakat luas.[16] Gambar berikut kiranya bisa membantu.

Gambar 6.

Strategi Resmi Keamanan Siber Finlandia[17]



[16] Lihat (Reza A.A Wattimena B. A., 2018)

[17] Dari (Cederberg, 2018)

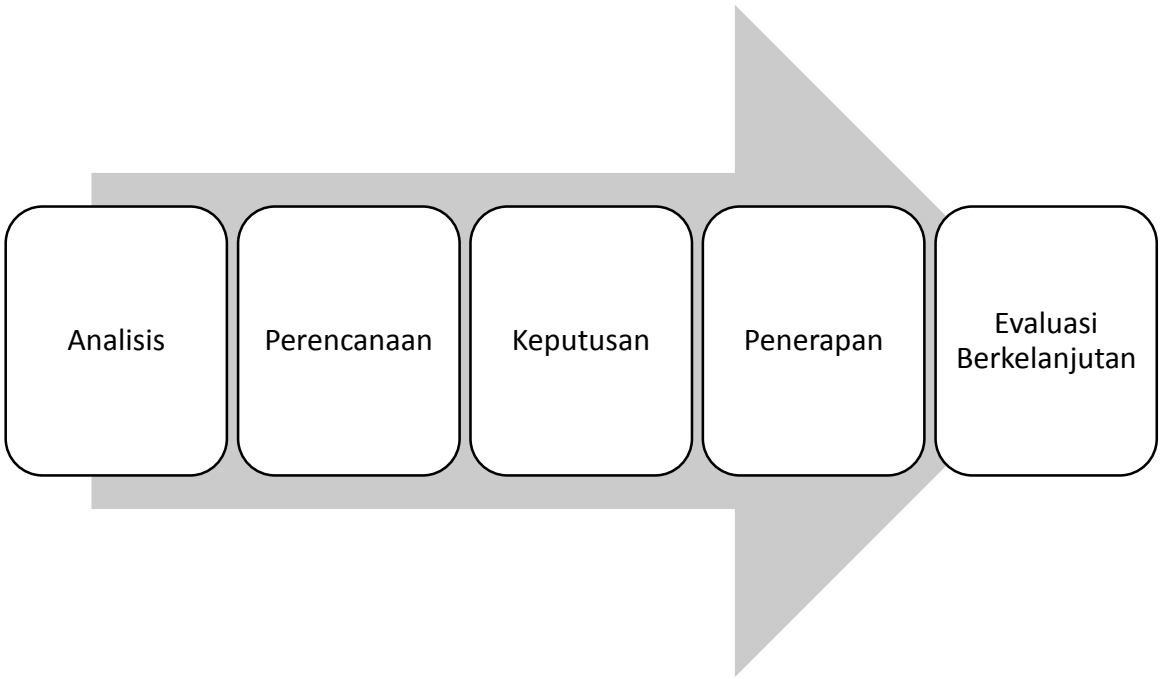
Keamanan siber adalah persoalan transdisipliner. Artinya, beragam bidang keilmuan yang saling melebur dibutuhkan untuk menopang wacana tersebut. Hal yang sama dianut oleh Finlandia di dalam mengelola keamanan siber mereka. Mereka melihat persoalan keamanan siber dari tujuh unsur, yakni unsur ketepatan aturan dan hukum, kepekaan melihat keadaan, penelitian yang menopang lahirnya pengetahuan-pengetahuan baru, kerja internasional, koordinasi yang efisien dan efektif antara berbagai lembaga yang ada, terutama antara pemerintah dan swasta, serta manajemen krisis yang efektif dan efisien, ketika serangan siber sudah terjadi, dan pemulihan yang cepat diperlukan.

Ketujuh unsur ini dipadukan dengan strategi keamanan siber menyeluruh yang menjadi kekuatan Finlandia. Pemerintah tetap memegang peranan terpenting, namun dalam kerja sama yang erat dengan militer, berbagai perusahaan swasta, lembaga penelitian dan universitas serta warga negara sebagai keseluruhan. Koordinasi dan berbagi informasi antara kelima unsur masyarakat tersebut memegang peranan kunci di dalam keamanan siber. Ini tentu menjadi semakin kokoh, jika kerja sama internasional antar negara dan juga dengan berbagai organisasi multinasional bisa berlangsung dengan baik.

Strategi siber Finlandia memiliki tujuan utama untuk membuat pembangunan yang berkelanjutan demi menjaga keamanan semua sistem siber di Finlandia secara efisien dan efektif. Strategi ini memiliki beberapa tahap. Yang pertama adalah analisis negara (*country analysis*), yakni upaya untuk menentukan keadaan sebuah negara di dalam menanggapi berbagai bentuk serangan siber. Dalam hal ini Finlandia melihat posisi mereka di hadapan komunitas internasional dalam kerja sama untuk mengembangkan sistem keamanan siber secara berkelanjutan.

Gambar 7.

Tahapan Strategi Siber Finlandia[18]



Langkah kedua adalah perencanaan tindakan. Ada tiga hal yang perlu menjadi perhatian, yakni kebutuhan nyata terkait dengan strategi keamanan siber yang ada, ketersediaan sumber daya dan kemampuan organisasi yang ada. Langkah ketiga adalah pembuatan keputusan. Keputusan dibuat dengan mempertimbangkan dua hal, yakni keadaan nyata di lapangan, dan prinsip-prinsip strategi siber yang dimiliki oleh pemerintah Finlandia.

Langkah keempat adalah penerapan rencanan yang sudah dibuat. Prinsip di dalam penerapan adalah komprehensibilitas. Artinya, seluruh unsur keamanan siber disentuh, termasuk antisipasi terhadap berbagai kemungkinan yang ada di masa depan. Prinsip kedua adalah prinsip delegasi dan koordinasi. Artinya, semua pihak bertanggung jawab atas wilayahnya masing-masing dalam koordinasi dengan berbagai lembaga lainnya. Pola pikir yang sama juga diterapkan dalam langkah kelima, yakni evaluasi yang meliputi kinerja seluruh lembaga terkait dengan keadaan di lapangan, dan prinsip-prinsip normatif keamanan siber Finlandia.

[18] Dari (Cederberg, 2018)

Di berbagai negara, keamanan siber adalah unsur penting dalam perkembangan politik dan ekonomi. Tidak hanya itu, keamanan siber merupakan unsur penting dalam kajian keamanan sebagai keseluruhan. Di abad 21 ini, keamanan siber merupakan kekuatan politik besar di dalam politik internasional. Ia memberikan efektivitas dan efisiensi yang tinggi di dalam berbagai bentuk pengolahan data terkait dengan kehidupan banyak orang, mulai dari persoalan hobi, ekonomi sampai dengan keamanan internasional.

2. Pelajaran untuk Indonesia

Strategi keamanan siber Finlandia adalah strategi yang bersifat menyeluruh. Dalam soal keamanan siber, Finlandia memang banyak menjadi contoh di tingkat internasional. Indonesia pun bisa banyak belajar dari pengalaman Finlandia. Setidaknya, ada empat hal yang penting untuk diperhatikan.

Pertama, Finlandia mengembangkan sistem siber dengan budaya sigap. Artinya, segala tugas dan tanggung jawab dilakukan dengan kepedulian dan kecepatan yang diperlukan. Sikap sigap dan tanggap lahir dari kesadaran akan pentingnya pekerjaan yang dilakukan tidak hanya bagi kebaikan diri sendiri, tetapi bagi kebaikan bersama. Budaya sigap semacam inilah yang amat lemah di Indonesia, sehingga berbagai bencana, baik alam ataupun buatan manusia, terus berulang, tanpa ada langkah pencegahan dan penangangan yang tepat.

Dua, budaya presisi juga amat penting dikembangkan, terutama dalam persoalan pengembangan sistem siber. Budaya presisi adalah budaya bertindak tepat dan akurat, sesuai dengan konteks yang ada. Tindakan sejalan dengan prinsip dan perjanjian yang telah disepakati, tidak kurang dan tidak lebih. Dalam hal ini, Indonesia amatlah kurang, sehingga berbagai upaya pencegahan bencana, termasuk berbagai bentuk serangan siber, amat mudah terjadi, dan merusak keamanan bersama.

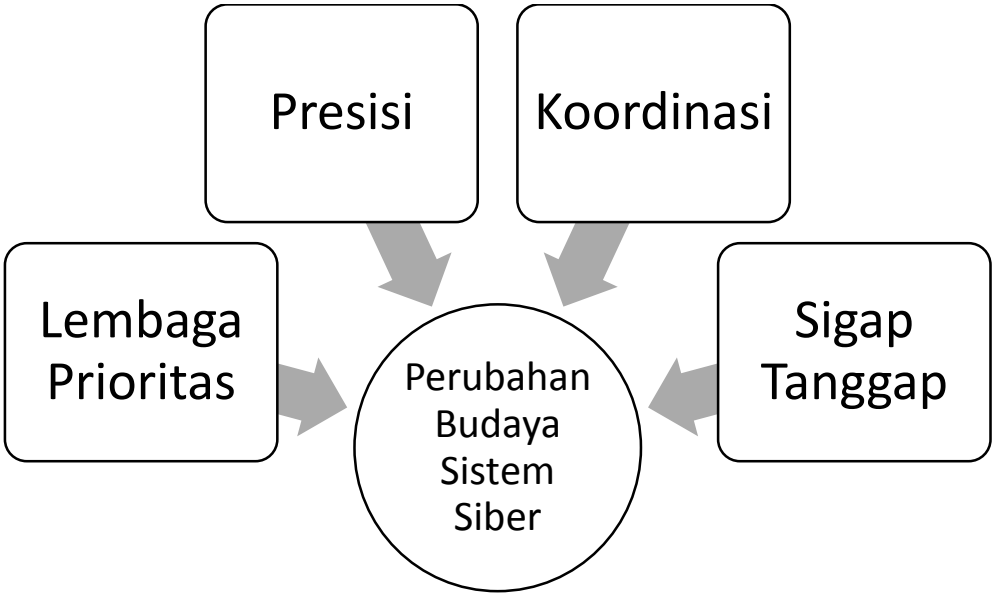
Tiga, belajar dari Finlandia, budaya koordinasi antar lembaga juga perlu dikembangkan. Di Indonesia, banyak institusi yang saling bersilangan tugas dan tanggung jawabnya. Ini menciptakan kebingungan yang besar, ketika diterapkan di lapangan. Ketika koordinasi berantakan, karena kebingungan tugas dan tanggung jawab, berbagai bencana yang terjadi tidak hanya tak tertangani, tetapi juga

menciptakan masalah-masalah baru. Ini menjadi hal yang amat penting untuk diperhatikan, terutama di dalam persoalan keamanan siber.

Keempat, belajar dari Finlandia, sistem tanggap keamanan siber di Indonesia harus memiliki ujung tombak yang jelas dalam bentuk satu lembaga resmi. Lembaga tersebut bekerja dalam koordinasi dengan berbagai lembaga lainnya, maupun dengan sektor swasta maupun masyarakat luas. Paradigma yang digunakan adalah paradigma integratif. Dengan mengembangkan koordinasi, prioritas kelembagaan, presisi dan budaya tanggap, keamanan siber di Indonesia bisa ditingkatkan.

Gambar 8.[19]

Perubahan Budaya Sistem Siber



Pengembangan sistem keamanan siber bukan hanya soal membangun sistem, tetapi juga melakukan perubahan budaya.[20] Semua ini merupakan bagian dari terciptanya kebaikan bersama dan kesejahteraan umum, seperti yang dicontohkan

[19] Rumusan penulis

[20] Lihat (Wattimena, Filsafat sebagai Revolusi Hidup, 2015)

oleh Finlandia. Keamanan siber akan memudahkan segala bentuk pengolahan informasi dan komunikasi berbagai pihak. Ini akan memberikan sumbangan besar untuk peningkatan mutu tata politik maupun ekonomi yang ada.

3. Kesimpulan

Di mata dunia, Finlandia adalah salah satu negara dengan strategi keamanan siber terbaik. Di abad 21 ini, keamanan siber menjadi persoalan yang amat penting dan kompleks untuk dipahami. Belajar dari Finlandia, setiap negara perlu mengembangkan strategi keamanan siber yang menyeluruh, beserta budaya yang menjadi latar belakangnya. Maka, peningkatan mutu keamanan siber juga berarti perubahan budaya itu sendiri, terutama dalam konteks pembelajaran untuk Indonesia. Dalam hal ini, empat nilai budaya, yakni budaya sigap, presisi, koordinasi dan prioriats kelembagaan, menjadi penting untuk diperhatikan dan dikembangkan, guna membangun strategi keamanan siber yang menyeluruh dan bermutu tinggi.

Daftar Acuan

Ardiyanti, H. (2014). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. *Politica Vol. 5 No. 1 Juni 2014*.

Cederberg, A. (2018). Comprehensive Cyber Security Approach: Finnish Model. In *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden.* Springer.

Charles J . Brooks, e. (2018). *Cybersecurity Essentials.* Sybex.

CSOOnline. (n.d.). Retrieved from https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

Forbes. (n.d.). Retrieved from https://www.forbes.com/sites/jeanmarcollagnier/2018/10/01/the-next-cyberattack-staying-ahead-of-hackers-is-becoming-a-greater-challenge/

Frey, S. (2018). How to Eliminate the Prevailing Ignorance and Complacency Around Cybersecurity. In S. F. Michael Bartsch, *Cybersecurity Best Practices:*

Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden (pp. 1-9). Wiesbaden: Springer.

Hansel, M. (2013). *International Beziehungen im Cyberspace: Macht, Institutionen und Wahrnehmung.* VS Verlag.

Harari, Y. N. (2018). *21 Lessons for the 21st Century.* Spiegel & Grau; 1st Edition edition.

Reza A.A Wattimena, Anak Agung Banyu Perwita (2017). Globalization: Citizenship and its Challenges, Cosmopolitanism as an Alternative Paradigm in International Relations. *Borderless Nation and Nations with Borders.* Yogyakarta: Gadjah Mada University.

Reza A.A Wattimena, Anak Agung Banyu Perwita (2017). Narrowing the Global Gap: Eco-Social Market Economy as New Perspective to Deal with Global Economic Inequality and Economic Insecurity in 21st Century. *Andalas Journal of International Studies Vol 6 No 1*.

Reza A.A Wattimena, Anak Agung Banyu Perwita (2017). Tolerance and Education: Developing Tolerance as a Way of Life in Indonesia. *The Ary Suta Center Series of Strategic Management, July 2017 Volume 38*.

Reza A.A Wattimena, Anak Agung Banyu Perwita (2018). *To Infinity and Beyond: Cosmopolitanism in International Relations.* Jakarta: Ary Suta Center.

Reza A.A Wattimena, Bustanul Arifin (2018). Melampaui Terorisme: Pendekatan Komprehensif untuk Memahami dan Menangkal Terorisme. *Mandala: Jurnal Ilmu Hubungan Internasional UPN Veteran Jakarta, 1*(1).

Wattimena, Reza A.A. (2012). *Filsafat Anti Korupsi.* Yogyakarta: Kanisius.

Wattimena, Reza A.A. (2015). *Filsafat sebagai Revolusi Hidup.* Kanisius.

Wattimena, Reza A.A. (2016, December). Retrieved from Rumah Filsafat: , https://rumahfilsafat.com/2016/11/04/belajarlah-sampai-ke-skandinavia/

Wattimena, Reza A.A. (2016). *Demokrasi: Dasar Filosofis dan Tantangannya.* Yogyakarta: Kanisius.

Wattimena, Reza A.A. (2018). Bisakah Perang Dihindari? *Ary Suta Center for Strategic Management*.