

PERTAHANAN KEAMANAN INFORMASI NASIONAL

Latar Belakang

Perkembangan dan kemajuan teknologi informasi dan komunikasi (TIK) telah merubah bukan hanya tatanan kehidupan dan cara interaksi sosial masyarakat namun lebih jauh lagi mendorong era peradaban baru dalam babak kehidupan manusia yang disebut dengan abad informasi.

Salah satu ciri utama era informasi ini adalah semakin banyaknya aktifitas sektor kehidupan manusia yang berlangsung dengan perantara atau bahkan hanya mungkin terjadi dengan adanya TIK. Sehingga di satu sisi ada ketergantungan sebagaimana dunia tergantung pada sumber energi, sumber pangan dan sumber daya strategis lainnya. Sehingga apabila terjadi sesuatu hal yang buruk di ranah maya (dunia lain yang tercipta karena TIK, misalnya Internet) maka dampaknya pun akan terasa secara langsung di dunia nyata.

Sebagaimana sumber daya penyokong peradaban dan kehidupan manusia yang lainnya, sepanjang sejarah selalu terjadi perlombaan penguasaan yang sebesar-besarnya sehingga barang siapa suatu bangsa yang memiliki sumber daya paling besar bisa menjadi penguasa dan menentukan kehidupan bangsa lainnya. Atau memiliki kemampuan bertahan yang lebih baik.

Dalam konteks yang positif, penguasaan sumber daya informasi yang lebih baik akan mampu mendorong peri kehidupan dan peradaban serta kesejahteraan suatu bangsa jadi lebih baik dan maju serta bergerak lebih cepat mengungguli bangsa lain. TIK menjadi modal bagi perubahan.

Dalam konteks yang negatif, semakin banyak nilai yang dihasilkan di dunia maya dan semakin tingginya tingkat ketergantungan manusia atau suatu bangsa, maka akan semakin besar pula resiko yang mengancam berupa aneka jenis kejahatan maupun upaya penguasaan sumber daya informasi yang dilakukan oleh bangsa lain dengan berbagai maksud dan tujuan. Sehingga amat penting bagi suatu bangsa yang telah makin intensif dan ekstensif memanfaatkan TIK untuk senantiasa mengamankan dan mempertahankan sumber daya informasi yang dimilikinya karena telah menjadi hajat hidup orang banyak yang dari hari ke hari akan menjadi semakin penting, bernilai tinggi dan bahkan merupakan asset vital.

Kejahatan Internet

ID-SIRTII mencatat sejumlah insiden sepanjang tahun 2009 dan awal 2010 yang dikategorikan sebagai kegiatan kriminal menurut peraturan perundangan yang berlaku terutama KUHP, UU No. 11/2008 Tentang ITE, UU No. 36/1999 Tentang Telekomunikasi dan ketentuan lainnya.

Kejadian yang menonjol antara lain: pencurian identitas dan data (sumber daya informasi) serta pembajakan akun (email, IM, social network). Kasus penyebaran malware dan malicious code (didominasi oleh virus lokal) yang disisipkan di dalam file dan web site serta phishing site. Fitnah, penistaan dan pencemaran nama baik. Fraud (penipuan, black dollar, nigerian scam). Spionase industri dan penyanderaan sumber daya informasi kritis. Cyber war atau saling serang karena alasan politis (ID vs MY, black campaign partai politik, calon anggota DPR). Penistaan keyakinan dan

penyebaran kabar bohong untuk tujuan provokasi politis maupun rekayasa ekonomi. Perjudian online, prostitusi dan human trafficking (tenaga kerja tidak resmi) serta child predator (menurut data Interpol, Indonesia terbesar di Asia Pasifik). Pornografi, peredaran narkoba dan underground economy (perdagangan komoditas tidak resmi). Cash out, penggelapan pajak dan money laundering. Serta aktivitas cyber terorisme terutama untuk tujuan propaganda, rekrutmen dan penggalangan dana.

Namun sebagian besar kasus belum dapat ditindaklanjuti oleh Kepolisian karena keterbatasan sumber daya dan akses, terutama menyangkut pemeriksaan oleh penegak hukum Indonesia kepada penyelenggara layanan asing di luar negeri walaupun UU ITE telah mengaturnya.

Upaya Pengamanan

Rata-rata jumlah insiden per hari pada tahun 2009 mencapai 1 juta insiden dan aktivitas ini cenderung akan semakin meningkat. Terutama pada situasi geopolitik tertentu seperti pemilu. 50% diantara insiden tersebut tergolong high priority alert. Sistem monitoring traffic ID-SIRTII sendiri terdiri dari 11 sensor yang meliputi hampir 70% traffic nasional, sehingga data dan informasi yang dihasilkan dapat digunakan untuk merepresentasikan profil traffic nasional.

Analisa data sistem monitoring traffic ID-SIRTII menunjukkan bahwa serangan ke infrastruktur Internet Indonesia sebagian besar disebabkan oleh kelemahan sistem dan aplikasi yang telah diketahui (common vulnerability). Penyebabnya adalah masih rendahnya kesadaran (kesadaran) para pengelola sistem dan pengguna aplikasi. Kemudian banyaknya penggunaan aplikasi tidak legal yang mengakibatkan tidak dilakukannya update atau patch untuk menutup kelemahan.

Web defacing rally (vandalism) dengan teknik eksploitasi database SQL masih menempati posisi tertinggi jumlah insiden disusul oleh serangan malware/malicious code terutama virus lokal dan phishing, scam serta SPAM yang juga mulai menyebar ke media selular (SMS dan MMS).

Insiden lainnya yang menjadi catatan khusus adalah serangan Distributed Denial of Service pada sistem Domain Name Service (DNS) CCTLD-ID yaitu domain .id terutama .co.id. Walaupun jarang terjadi akan tetapi implikasinya sangat luas. Pada pertengahan tahun 2009 domain .co.id sempat drop selama 4 hari akibat serangan ini. Hal ini menunjukkan adanya kelemahan mendasar dalam sistem DNS CCTLD-ID yang perlu segera diperbaiki mengingat domain .id merupakan salah satu infrastruktur vital Internet Indonesia. Mitigasi insiden ini harus melibatkan banyak pihak terkait karena jaringan DNS ini tersebar.

Ternyata juga diketahui bahwa sekitar 30% hingga 40% utilisasi traffic Internet internasional digunakan untuk akses konten negatif terutama pornografi, warez activity dan konten multimedia illegal. Dimana dampak ikutan akses konten negatif ini mengakibatkan tingginya insiden akibat malware/malicious code. Menurut data statistik forum keamanan Internet lebih dari 40% malicous code disebarkan menumpang pada material konten negatif dan sisanya melalui SPAM. ID-SIRTII juga telah melakukan uji random sampling bersama Tim dari JPCERT/APCERT dengan melakukan analisa terhadap produk warez, pornografi dan konten multimedia illegal di pasaran Indonesia. Hasilnya positif sebagian (30%) diantaranya memang mengandung malware/malicious code.

Penyebab insiden tertinggi lainnya adalah diakibatkan oleh kesalahan prosedur pengamanan dan kelalaian pengelola sistem. Kemudian akibat pengabaian dan ketiadaan prosedur serta pengelolaan sistem pengamanan yang memadai. Kasus social engineering terutama untuk mendapatkan hak akses dari para pejabat perusahaan atau operator dan pengelola sistem semakin banyak terjadi, akan tetapi sangat jarang dilaporkan karena dianggap dapat mengancam kredibilitas perusahaan apabila sampai informasi mengenai insiden tersebut terpapar ke publik.

Information gathering, termasuk teknik trashing – mencari data informasi rahasia dan sensitif melalui media bekas seperti portable external storage, CD/DVD dan kertas kerja yang tidak dihancurkan, penghapusan yang tidak sempurna dan tidak mengikuti prosedur pengamanan (secure disposal) untuk perangkat yang sudah habis masa pakainya serta kebiasaan berganti perangkat gadget tanpa mengikuti prosedur screening yang memadai. Banyak kasus kebocoran data perusahaan dan penyebaran data privacy dengan tujuan pencemaran akibat kurangnya kesadaran pengguna terhadap prosedur pengamanan perangkat gadget dan komputer portabel.

ID-SIRTII juga telah mengadakan survey random sampling tentang kesiapan sistem dan prosedur terhadap sejumlah perusahaan serta instansi pemerintah di berbagai sektor yang bisa dianggap strategis dan kritical. Hasilnya, meskipun sebagian besar telah memiliki instrumen pengamanan namun banyak sekali kelemahan akibat sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (self protection). Semua ini mengakibatkan tingginya angka insiden yang tidak disadari oleh pemilik sistem.

Untuk membuktikan hasil survey tersebut, ID-SIRTII juga melakukan analisa terhadap aktivitas pasar underground economy. Hasilnya cukup bersesuaian dengan premise awal dimana informasi sensitif perusahaan dan data-data pribadi rahasia (termasuk identitas, nomor rekening, PIN dan password) adalah komoditas yang paling aktif diperdagangkan dan diminati. Patut diduga bahwa kegiatan ini mengarah kepada spionase industri baik domestik, regional maupun internasional.

Di masa depan, pemerintah perlu menerbitkan suatu regulasi dan panduan prosedur pengamanan data dan informasi sensitif terutama untuk instansi strategis dan vital.

Perang Informasi

Cyberwarfare (cyberwar), adalah penggunaan teknologi komputer dan internet (TIK) untuk melakukan perang di dunia maya. Pelaku cyberwar saling bersaing untuk menguasai dan memanfaatkan sumber daya teknologi serta informasi yang ada di dalamnya untuk menyerang, menghancurkan, menyesatkan, mempengaruhi, menyandera, mengurangi, menghilangkan, mengalihkan, mengganggu, menghentikan komunikasi, arus informasi dan isinya serta berbagai tindakan lain yang mengakibatkan kerugian dan melemahkan lawan.

Seringkali kegiatan ini dilakukan secara anonim, rahasia, acak, terselubung, terus-menerus dalam waktu yang lama dan tidak secara langsung atau terang-terangan serta memanfaatkan potensi yang tidak saling terkait sehingga sulit diketahui siapakah musuh yang sesungguhnya dan apa tujuannya. Batasan fisik di dunia nyata seperti wilayah negara tidak berlaku di dunia nyata sehingga upaya pencegahan, merespon dan menanggulangi kejadian cyberwar sulit disikapi oleh sistem hukum

yang berlaku. Sehingga kerjasama antar negara menjadi syarat mutlak untuk dapat melacak, mengungkapkan dan menindak pelakunya.

Cyberspaces (dunia maya) kini telah menjadi tempat potensial untuk menjadi medan pertempuran dan konflik tradisional maupun khusus. Bukan hanya pihak yang mewakili entitas suatu negara namun juga kelompok masyarakat lainnya yang saling berseteru. Mereka saling berhadapan melalui ajang perdebatan, adu argumentasi, penyebaran upaya dominasi informasi hingga kegiatan yang bersifat destruktif seperti web defacing rally sebagai cara propaganda dan intimidasi atau yang lebih berat lagi. Perseteruan ini tidak hanya melibatkan pelaku amatir tapi juga mereka yang punya keterampilan dan kemampuan khusus bahkan banyak kelompok profesional yang menawarkan jasa layaknya tentara bayaran.

Keterampilan yang dimiliki misalnya di bidang strategi keamanan dan pengamanan serta serangan informasi (information security and warfare), ahli meretas (hacking), spionase (espionage), forensik digital (digital forensic) dan analis keamanan jaringan (network security analyst) dlsb. Alat bantu (tools) dan pengetahuan menggunakan sehingga dapat digunakan sebagai senjata untuk melakukan suatu serangan (cyber attack) yang mengawali suatu cyberwar juga dapat dengan mudah diperoleh di internet itu sendiri. Sehingga keahlian ini tidak bersifat eksklusif.

Kemampuan perang itu kini bukan hanya bisa dikuasai kelompok militer, keamanan atau penegak hukum sebagaimana dalam kehidupan nyata, tapi juga justru lebih banyak dikuasai oleh sipil. Terutama mereka yang bekerja di bidang ini, para hobbyist maupun orang berbakat yang khusus direkrut dan dilatih untuk tujuan itu. Industri keamanan informasi juga menyediakan pelatihan, pendidikan serta sertifikasi keahlian untuk menghasilkan sumber daya manusia walaupun pada sisi lainnya jalur informal, otodidak maupun kelompok pembelajar juga lebih banyak diminati sebagai tempat untuk mendapatkan dan berbagi ilmu.

Perang informasi berupa kampanye, propaganda dan agitasi dengan tujuan untuk membentuk opini publik dan persepsi internasional terhadap suatu kepentingan (interest) suatu kelompok di internet ternyata bisa sangat berpengaruh dan efektif serta mengakibatkan dampak di dalam kehidupan nyata. Indonesia sebenarnya punya banyak pengalaman terkait dengan masalah ini. Pada tahun 1998 gerakan reformasi melakukan perang opini melawan media konvensional yang terkontrol oleh kekuasaan Pemerintah ketika itu, penggalangan dukungan dan koordinasi melalui saluran internet email, mailing list, chatting (IRC), forum dan web site. Hal yang sama ternyata dilakukan oleh kelompok pro kemerdekaan Timor Timur dan mereka mendapatkan hasil kemenangan akibat opini dan persepsi internasional yang gagal diantisipasi oleh propaganda Indonesia. Hal ini ternyata berulang kembali dalam kasus perebutan Pulau Sipadan dan Pulau Ligitan antara Indonesia dengan Malaysia. Hakim Mahkamah Arbitrase Internasional memutuskan kedua pulau itu jatuh ke tangan Malaysia atas dasar alasan "eksistensi" yang salah satunya dilihat dari bukti adanya informasi, promosi, pemetaan, foto, publikasi, artikel, catatan dan segala jenisnya yang sistematis, terstruktur diterbitkan atas nama Malaysia dan dikenal secara internasional (karena berbahasa Inggris) dimana salah satunya media internet berperan sangat besar dalam menyebarkan. Mahkamah menilai bahwa Malaysia lebih serius melakukan berbagai hal, pengembangan dan publikasi sebagai "pemilik" dibandingkan Indonesia yang pasif.

Jejak sejarah peristiwa tersebut sampai saat ini masih bisa ditelusuri di Internet.

Konteks Internasional

Malaysia adalah salah satu contoh negara yang secara serius, sistematis, strategis memanfaatkan kemampuan perang informasinya untuk mendapatkan kemenangan moral di pergaulan internasional, mendapatkan pencitraan positif dan keuntungan ekonomi dalam mendapatkan berbagai peluang yang meningkatkan keunggulan dan daya saing mereka. Dalam sejumlah kasus klaim terhadap unsur dan material seni budaya asal Indonesia (lagu Rasa Sayange, Tari Pendet, Reog, kain Tenun dan Batik) sebagai komoditas seni dan budaya serta untuk meraih keunggulan di sektor pariwisata, pihak Malaysia melakukan perang informasi yang sistematis dalam jangka waktu lama melalui saluran konvensional dan media baru seperti Internet. Jargon "Malaysia Truly Asia" dalam 10 tahun terakhir sangat dikenal dunia dengan hasil secara statistik meningkatkan posisi Malaysia dalam dunia seni budaya pariwisata mengungguli Thailand dan Indonesia.

Singapura adalah salah satu tetangga Indonesia yang juga melakukan kampanye sejenis melalui media Internet yang uniknya justru menyasar pangsa pasar dari Indonesia. Sejumlah laporan statistik menunjukkan bahwa 70% konsumen wisata belanja Singapura adalah berasal dari Indonesia dan sebagian besar mendapatkan informasinya melalui Internet dan atau media elektronik. Sangat efektif.

Kecenderungan saat ini dalam perang informasi terutama di Internet adalah untuk tujuan ekonomi, penguasaan sumber daya milik lawan secara tidak sah, persaingan dan spionase industri. China dan Rusia adalah dua entitas yang dianggap memimpin serangan-serangan dengan motif ekonomi tidak sah tersebut ke seluruh dunia. Para pelaku konon mendapatkan dukungan tidak resmi dan terselubung atau difasilitasi secara tidak langsung oleh pemerintah. Bahkan Amerika Serikat yang menjadi target utama sampai harus membentuk Task Force khusus untuk menanggulangi bahaya spionase industri dan perang informasi dari China dan Rusia. Sudah banyak sekali terjadi kasus pembajakan, pencurian atau kebocoran data dan informasi bisnis, sumber daya ekonomi strategis serta kekayaan intelektual jatuh ke pihak kriminal dan tersebar pada sebuah pasar yang disebut "underground market" yang kebanyakan memang telah dideteksi dijalankan dari pedalaman China dan Rusia.

Secara umum perang ideologi dalam peta dunia informasi sudah bukan lagi suatu yang riil bahkan absurd untuk diwaspadai sebagai sebuah ancaman bagi negara atau bangsa sebagaimana era perang dingin pada akhir abad 20. Motif perang kini sudah sangat jauh bergeser kembali seperti pada era imperialisme dunia, kepentingan saling menguasai secara ekonomi dan kepemilikan sumber daya kini jauh lebih menonjol sebagai suatu alasan ofensif dibandingkan ideologi.

Pergeseran ini juga terjadi sebagai akibat semakin meleburnya batas wilayah teritorial adat istiadat budaya bahkan hukum di Internet sehingga menjadi sebuah kampung dunia maya yang universal. Paham, ide, keyakinan dan kepentingan yang sifatnya ego sektoral non ekonomi kini sudah tidak laku untuk ditawarkan sebagai daya penarik simpati atau keberpihakan suatu kelompok pada kelompok lainnya. Walaupun ideologi, paham hingga ekstrimisme juga ikut berpindah dan berkembang di dunia maya, namun kekuatan materialistik penguasaan sumber daya serta keunggulan ekonomi pada saat ini jauh lebih punya pengaruh dan menjadi tujuan perebutan oleh kekuatan-kekuatan dunia untuk saling bersaing mendapatkannya.

Inilah masa depan dunia. Dalam bahasa populer: ujung-ujungnya duit (UUD).

Serangan Terhadap Infrastruktur

Di Internet juga terjadi serangan yang bertujuan melumpuhkan infrastruktur dan menghancurkan sumber daya lawan. Bersifat destruktif secara fisik, mencederai bahkan mematikan, mengancam keselamatan jiwa dan harta benda. Ini juga patut diwaspadai karena pelakunya bisa beraneka ragam dan saling bekerja sama walaupun kepentingannya berbeda. Apakah itu politik, ideologi, ekonomi atau kriminal serta kombinasi hal tersebut.

Banyak sekali jenis serangan masif yang mematikan seperti DDOS (distributed denial of service). Biasanya serangan semacam ini direncanakan dengan baik dan dilakukan secara terstruktur dengan satu strategi operasional yang matang bahkan dilengkapi dengan kemampuan proteksi dari serangan balik, pelacakan dan prosedur cover up untuk menghilangkan jejak. Biasanya serangan ini didahului dengan upaya menyebar malware bots (pasukan aplikasi jahat semacam virus - malicious code - yang akan menginfeksi sejumlah besar komputer di seluruh dunia dan dikendalikan penyerang - attacker - sebagai zombie - titik penyerangan ke infrastruktur atau sumber daya lawan). Bots ini biasanya akan berdiam diri (dormant) di komputer yang terinfeksi dan sulit dideteksi oleh tools anti malware dan anti viurs. Pada saatnya dia dapat diperintahkan untuk aktif dan menyerang sasaran yang sudah ditentukan (targetted) secara bersama-sama (distributed) sehingga dapat mengakibatkan kerusakan dan kerugian material yang nyata.

Negara yang pernah menjadi korban serangan botnet adalah Estonia, pecahan Uni Soviet di Eropa Timur pada tahun 2007. Latar belakang serangan adalah masalah SARA, ketidakpuasan etnik Rusia atas dipindahkannya patung Pahlawan Lenin dari pusat kota ke Taman Makam Pahlawan. 1/2 populasi Estonia keturunan Rusia melakukan kerusuhan dan penjarahan selama 2 hari yang segera diatasi petugas keamanan. Akan tetapi, serangan kemudian beralih dan berlanjut ke dunia maya. Isu pelecehan etnik melalui dipindahkannya patung pahlawan Lenin ini menyebar hingga ke Rusia dan menyulut aksi solidaritas dari komunitas underground (hacker). Dalam beberapa hari sejumlah bots disebar melalui berbagai saluran dan berhasil menginfeksi jutaan komputer di seluruh dunia yang perlahan menghujani infrastruktur Internet Estonia dengan paket sampah sehingga mengakibatkan kelumpuhan jaringan. Akibatnya sistem jaringan listrik, gas, transportasi, keuangan/perbankan, layanan publik dan media yang berbasis Internet lumpuh. Kerusuhan dan penjarahan kedua terjadi akibat rakyat lapar tidak bisa membeli makanan dan layanan publik tidak tersedia. Setelah beberapa hari kerusuhan tidak terkendali, Menteri Pertahanan Estonia resmi meminta komunitas internasional untuk membantu menghentikan serangan (cyber attack) tersebut karena titik asal serangan dari seluruh dunia dan Indonesia salah satu yang terbesar (akibat banyak komputer menggunakan aplikasi bajakan yang tidak update sehingga mudah diinfeksi program jahat - malware dan bots).

Dengan terjadinya peristiwa Estonia under attack pada tahun 2007 itu maka dunia disadarkan oleh kenyataan adanya ancaman serangan dalam konteks cyberwar yang sangat mungkin akan melibatkan sejumlah besar negara-negara yang sebenarnya tidak ikut punya kepentingan terhadap alasan-alasan konflik tersebut. Misalnya peran serta Indonesia dalam kasus Estonia di atas.

Selain itu, konflik yang berujung serangan melibatkan sejumlah negara yang secara tradisional, politik dan sosial budaya memiliki sejarah sengketa bisa menjadi motif terjadinya peperangan dilakukan oleh kelompok-kelompok non pemerintah. Sebagai contoh adalah antara Indonesia vs Malaysia, Indonesia vs Australia, Indonesia vs Timor Timur dan Portugal (pada tahun 1996 dan 1997 Indonesia menyerang sistem domain .pt milik Portugal sehingga terhapus dari Internet) pada periode acak yang bisa terjadi sepanjang tahun. Demikian juga antara China vs Korea, China vs Jepang, Korea vs Jepang, Taiwan vs China dlsb. yang rutin terjadi pada waktu tertentu pada saat misalnya menjelang peringatan Perang Dunia ke II. Tahun 2009 sistem domain .co.id milik Indonesia juga mengalami serangan masif yang diduga dipicu oleh kasus provokasi perairan Ambalat oleh Malaysia walaupun terdeteksi asal serangan dari China dan Amerika Serikat.

Di Indonesia, semakin banyak infrastruktur strategis dan layanan publik yang telah semakin bergantung pada sistem informasi, teknologi dan jaringan Internet sehingga rentan terhadap ancaman, gangguan dan serangan. Sistem transmisi dan distribusi energi (listrik, pertambangan dan energi/minyak dan gas), sistem pertahanan udara, sistem transportasi (darat, laut, udara) yang bergantung dengan teknologi navigasi serta pengendalian yang kini juga berbasis Internet, layanan publik pemerintahan dan sipil termasuk bea cukai dan pajak, pemantauan dan pengendalian lalu lintas, hingga industri jasa dan layanan keuangan, perbankan (ebanking, phone banking, mobile banking) dlsb. Potensi chaos akibat kegagalan sistem dan fraud sangat tinggi dan sejumlah kasus telah terjadi dengan kecenderungan peningkatan signifikan.

Kendati demikian, langkah antisipasi pencegahan, pengamanan dan penanggulangan masih sangat minim bahkan banyak diantara entitas penyelenggara negara yang seharusnya bertanggung jawab justru belum memiliki kesadaran yang memadai.

Pertahanan Informasi

Ancaman perang informasi dan cyber attack akan semakin meningkat dan menjadi medan pertempuran utama di masa mendatang. Sehingga setiap negara dan entitas di Internet merasa perlu untuk memiliki kemampuan pertahanan dan pengamanan. Salah satunya adalah dengan mengandalkan kemampuan intelejen dan pengawasan (monitoring) terhadap dunia maya (cyberspace) untuk mendeteksi sejak dini segala macam potensi ancaman, gangguan hingga serangan sehingga dapat melakukan antisipasi dan pencegahan serta penanggulangan (mitigasi) pasca insiden.

Banyak negara kini telah membangun inisiatif National Cyber Security yang bertugas untuk menyusun aturan dan kebijakan nasional menyangkut upaya pengamanan sumber daya informasi, perlindungan infrastruktur strategis dan mengembangkan kemampuan respon serta koordinasi lintas sektoral. Serta memiliki tim respon insiden yang disebut dengan CERT (Computer Emergency Response Team) atau CSIRT (Computer Security Incident Response Team) serta sekaligus berfungsi sebagai CC (Coordination Center) untuk berkolaborasi dengan inisiatif sejenis di sektor lokal maupun regional dan dunia internasional. CC juga bertugas untuk konsolidasi semua potensi kekuatan pengamanan dan pertahanan di semua sektor strategis.

Model pertahanan yang umumnya dikembangkan menerapkan koridor (frame work) standar pengamanan baku dan prosedur operasional untuk setiap sektor terutama infrastruktur strategis yang terus-menerus dievaluasi dan ditingkatkan. Selain itu juga dilakukan kontra intelejen (menangkal aksi intelejen lawan) dilakukan inisiatif

yang disebut pertahanan proaktif (proactive defense) yaitu upaya yang meliputi intelejen (data mining, examining, analysis), surveillance (termasuk social network and corporate analysis), targeted profiling, identification and credential, human operative dan penetrasi terhadap target potensial lawan untuk mengenali sebanyak mungkin kemampuan, sumber daya dan menemukan kelemahan serta antisipasinya bila harus berhadapan dengan entitas tersebut.

Sebagaimana sistem pertahanan lainnya, fungsi kegunaan dan manfaatnya baru dapat dirasakan apabila telah terjadi. Akan tetapi seiring dengan semakin banyak anggota masyarakat yang beraktifitas dan berinteraksi di Internet maka nilai (value) dunia maya (cyber space) akan semakin tinggi. Dan dimana ada suatu nilai maka bisa dipastikan akan selalu ada ancaman dan resiko yang menyertainya. Dengan kondisi tingkat penetrasi Internet reguler telah mencapai 45 juta orang (pesimistik) pada awal tahun 2010 dan akan mencapai 150 juta pada tahun 2015, 175 juta penyebaran nomor selular pada akhir tahun 2009 dan telah menjangkau semua (5.748) kecamatan di seluruh Indonesia (Internet ready), dengan total traffic telah mencapai 45 Gbit/s (internasional) dan 25 Gbit/s (lokal) maka tidak diragukan lagi bahwa teknologi dan layanan ini telah menjadi kebutuhan mendasar dan vital. Bila terjadi insiden, kemungkinan chaos sangat besar demikian juga dampaknya.

Indonesia belum memiliki kebijakan dan kemampuan pertahanan informasi yang memadai bukan hanya untuk menghadapi serangan cyber secara pasif maupun ofensif melainkan juga sistem cadangan (backup) dan retensi data serta informasi strategis yang mampu dengan cepat dipulihkan (recovery) dalam situasi darurat. Termasuk misalnya akibat bencana alam (natural disaster). Dari pengalaman saat terjadi sejumlah bencana, ternyata data dan informasi penting baik sipil seperti data kependudukan, pertanahan, pemerintahan, perbankan dsb. serta militer keamanan seperti persenjataan, perlengkapan, dokumen rahasia tidak memiliki cadangan atau backup sehingga tidak mungkin dipulihkan dengan cepat dalam proses rehabilitasi.

Tidak cukup hanya perlindungan dan pencadangan data maupun informasi ternyata dalam konsep pertahanan suatu negara harus memiliki infrastruktur cadangan yang bersifat rahasia, tertutup. Sistem ini harus didesain memiliki kemampuan bertahan dan berfungsi dalam kondisi darurat dibawah tekanan serangan maupun akibat bencana. Sehingga sistem ini dapat diandalkan untuk alternatif saluran konsolidasi.

Adalah sangat penting untuk menyampaikan pemahaman, perkembangan situasi serta berbagi pengetahuan dan sumber daya yang ada di ID-SIRTII kepada setiap entitas yang memiliki potensi pertahanan dan pengamanan informasi di Indonesia agar secepatnya membangun kesadaran dan kemampuan kemampuan yang nyata dalam menjawab ancaman perang informasi dan tantangan dunia ke depan serta demi melindungi kepentingan negara, keselamatan dan kesejahteraan bangsa.

M. Salahuddin. Penulis adalah Wakil Ketua Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII), sebuah lembaga kuasi pemerintahan di bidang keamanan Internet yang didirikan oleh komunitas dan industri Internet di Indonesia dan difasilitasi oleh Departemen Komunikasi dan Informatika Republik Indonesia. Lembaga negara ini berfungsi sebagai National CERT/CSIRT/CC dan saat ini telah resmi terdaftar sebagai anggota APCERT (Asia Pacific Computer Emergency Response Team).