Bagaimana Standar EU NIS Platform, NIST, dan IETF Menjadi Dinding Penghambat dalam Information Sharing

Maulana Yusuf Fathany (23214016)

Mikroelektronika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Indonesia
myfathany@s.itb.ac.id

Abstrak

Penanganan secara global melalui *information sharing* dipandang mampu untuk mempercepat proses pemulihan dan deteksi dini akan sebuah ancaman. Namun belum terciptanya sebuah kesepakatan tingkat dunia menjadikan dinding penghambat dalam skema *information sharing* dari sektor kebijakan. Hal tersebut juga secara langsung berdampak pada sektor teknis dan tata kelola, dimana penentuan infrastruktur dan konten berikut metoda pendukung pertukaran informasi masih bersifat lokal. Sehingga beberapa upaya inisiatif telah dilakukan untuk mendukung proses *information sharing* yang terstruktur, aman, dan otomatis. Diantaranya adalah teknik kolaborasi CybOS, STIX, dan TAXII oleh US-CERT. Sedangkan pada sektor kebijakan global masih dalam proses perancangan, sehingga kepaduan antara EU-NIS, NIST, dan IETF diharapkan dapat mengurangi efek dinding penghambat dalam skema *information sharing* tingkat dunia.

Kata kunci— *information sharing*, EU-NIS, NIST, IETF

1 Pendahuluan

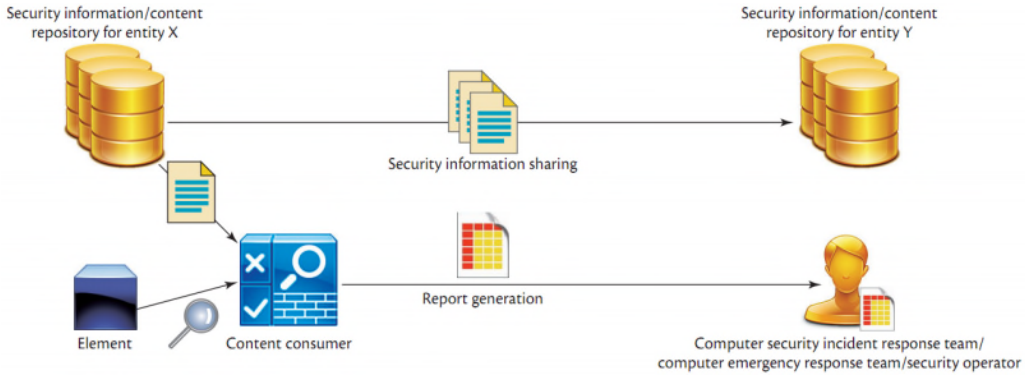
Pesatnya perkembangan internet tidak selaras dengan laju pengembangan bidang keamanan informasi. Selama ini penangamanan ancaman *cyber* dilakukan secara individual tanpa kolaborasi global [1][2]. Sehingga penanganan ancaman *cyber* tersebut kurang efisien dalam penanganannya [3]. Penanganan secara global melalui *information sharing* dipandang mampu untuk mempercepat proses pemulihan dan deteksi dini akan

sebuah ancaman. Informasi merupakan aset yang sangat penting saat ini, dimana isu keamanan informasi dan manajemen pengangan insiden dianggap sebagai solusi yang menjadi topik sentral. Jaminan kemanan informasi sebuah organisasi bergantung pada implementasi kebijakan keamanan dan latihan yang dilakukan organisasi tersebut [4].

Menurut dokumen SP 800-30, ancaman *cyber* adalah setiap keadaan atau peristiwa dengan potensi yang menghasilkan dampak negatif bagi operasi organisasi (termasuk misi, fungsi, nilai jual, atau reputasi), aset organisasi, individu, organisasi lain, atau negara melalui sistem informasi dengan akses yang tidak sah, perusakan, pengungkapan, atau modifikasi informasi, ataupun penolakan layanan [5].

Beberapa skema *information sharing* juga telah diterapkan pada berbagai sistem seperti pada sistem *Supply Chain Management* (SCM) berbasis internet [4], lingkungan virtual dengan konsep *Virtual Multi-Agency Team Environment* (VMART) [6], dan pada *Product Lifecycle Management* (PLM) [7].

Sedangkan manfaat dari *information sharing* meliputi: meningkatnya kewaspadaan dan keamanan; meningkatnya pemahaman akan ancaman; pematangan pengetahuan; terbentuknya imunitas; dan meningkatnya ketangkasan organisasi-organisasi yang tergabung dalam komunitas tersebut dalam pertahanannya [8]. Namun masalah yang dihadapi saat ini meliputi: proses penanganan yang masih dilakukan secara manual (membutuhkan operator manusia) untuk menyaring informasi baik dari web atau dalam bentuk PDF [9]; sumber yang berbeda menghasilkan tingkat konteks, deskripsi, atau istilah yang berbeda pula; dan beberapa organisasi telah menyediakan perangkat otomasi yang diperuntukkan hanya untuk komunitasnya saja.



Gambar 1: Data arsitektur dari keamanan informasi [10]

Langkah dini yang umum dilakukan ketika terjadi insiden adalah identifikasi dan karakterisasi sebuah insiden. Karakterisasi ancaman yang terjadi perlu adanya otomasi

perangkat sebagai perangkat yang mampu mengambil alih proses pertukaran informasi yang efisien [2]. Sehingga muncul sebuah inisiatif untuk mengaktifkan data *Indicator of Compromise* (IOC) yang dipertukarkan dalam sebuah format yang umum (Misalnya CybOX dan OpenIOC) [9]. Gambar 1 menunjukkan arsitektur otomasi *data-sharing* dimana entitasnya berbagi informasi keamanan. Perangkat otomatis dapat menggunakan informasi ini untuk menegakkan kebijakan keamanan, alamat insiden, dan mengevaluasi infrastruktur [10].

Dalam berbagi informasi, setidaknya dapat memberikan pengetahuan tambahan akan penebar ancaman. Hal tersebut dapat terjadi jika informasi yang didapatkan berasal dari berbagai sumber. Kembali pada permasalahan pertama bahwa proses pertukaran informasi itu juga membutuhkan sumber daya waktu maupun tenaga. Langkah awal sebelum masuk pada pertukaran informasi adalah karakterisasi ancaman yang terjadi. Ada banyak upaya dilakukan untuk mengkarakterisasi ancaman hingga perbaikan dasar [9]. Beberapa perangkat alternatif yang dapat digunakan sebagai upaya awal seperti CybOX, STIX, maupun TAXII diusulkan dalam makalah ini.

Beralih pada permasalahan kedua, dimana sumber yang berbeda menghasilkan tingkat konteks, deskripsi, atau istilah yang berbeda pula. Dalam konteks ini keberagaman standar yang dipakai menjadi dinding penghambat dalam *information sharing*. Selaras dengan permasalahan terakhir dimana beberapa organisasi telah menyediakan perangkat otomasi yang diperuntukkan hanya untuk komunitasnya saja yang memungkinkan nilai dari tujuan peningkatan interoperabilitas menjadi menurun. Masalah-masalah tersebut bersinggungan langsung dengan sektor teknis, kebijakan, dan tata kelola.

Beberapa organisasi telah mencoba untuk menerbitkan standar *information sharing* pada tingkat kewilayahan dengan versinya masing-masing. Adapun standar yang telah ada seperti *European Union Network and Information Security* (EU-NIS) pada tingkat benua dan *US National Institute of Standards and Technology* (US-NIST) pada tingkat negara perserikatan. Selain itu komunitas dunia yang bersifat terbuka seperti *Internet Engineering Task Force* (IETF) juga mendeskripsikan pentingnya konsep sharing dan pertukaran informasi tentang ancaman *cyber*. Sehingga makalah ini akan membahas tentang irisan-irisan yang mungkin untuk penyeragaman standar dalam *information sharing*.

2 Perangkat Alternatif *Information Sharing*

Terdapat banyak perangkat alternatif yang mendukung proses pertukaran informasi seperti yang terlihat pada tabel 1 [10]. Ketiga perangkat alternatif ini merupakan produk dari MITRE. Pemilihan ketiga perangkat berikut bertujuan untuk menambahkan pengetahuan tentang upaya yang telah dilakukan untuk mewujudkan proses pertukaran informasi yang terpercaya dan aman. Pemilihan juga bukan didasarkan pada kecenderungan faktor geografis asal dari ketiga perangkat tersebut, meskipun pada kenyataannya US-CERT menggunakan ketiganya sebagai teknik pertukaran informasi.

Tabel 1: Fungsi dan Ragam Perangkat Pertukaran Informasi [10]

Scheme	Purpose	Similarities
Trusted Automated Exchange of Indicator Information (TAXII)	Threat *information sharing* (messages, queries, transport, and content binding)	RID and Extensible Messaging and Presence Protocol (XMPP)
Real-Time Inter-network Defense (RID)	Incident (IODEF) transport	TAXII and XMPP
Structured Threat Information Expression (STIX)	Information representation and grouping incorporating other scemata	
Cyber Observable Expression (CybOX)	Threat events and machine property representation	OVAL and OpenIOC
Common Attack Pattern Enumeration and Classification	Malware behaviors, artifacts,and attack pattern representation	
Malware Attribute Enumeration and Characterization (MAEC)	Attack pattern description	MMDEF, OpenIOC and Yara
Open Vulnerability and Assessment Language (OVAL)	System information representation, state representation, and assessment reporting	CybOX and OpenIOC
Extensible Configuration Checklist Description Format (XCCDF)	Security checklist and benchmark representation	
Common Platform Enumeration (CPE)	Hardware and software asset description and identification	SWID
Common Vulnerabilities and Exposures	Public security vulnerability and exposure dictionary	
Common Vulnerability Scoring System	Security vulnerability scoring system	
Common Configuration Enumeration	Security configuration issue dictionary	
Common Configuration Scoring System (CCSS)	Security configuration scoring system	
Open Checklist Interactive Language	Human question/answer interpretation and trnsformation	
Common Weakness Enumeration	Common software weakness dictionary	
Common Weakness Scoring System (CWSS)	Sofware weakness scoring system	
Incident Object Description Exchange Format (IODEF)	Basic compromise indicator and incident sharing	VERIS
Malware Metadata Exchange Format (MMDEF)	Malware description	MAEC
Common Vulnerability Reporting Framework	Vulnerability description	OVAL
Open Indicators of Compromise (OpenIOC)	Indicators of compromise description	CybOX, OVAL, and more
Software identification (SWID) tags	Installed software descriptors	CPE
Vocabulary for Event Recording and Incident Sharing (VERIS)	Malware property and packet representation	IODEF
Yara	Incident reporting and analysis	Malware signature software

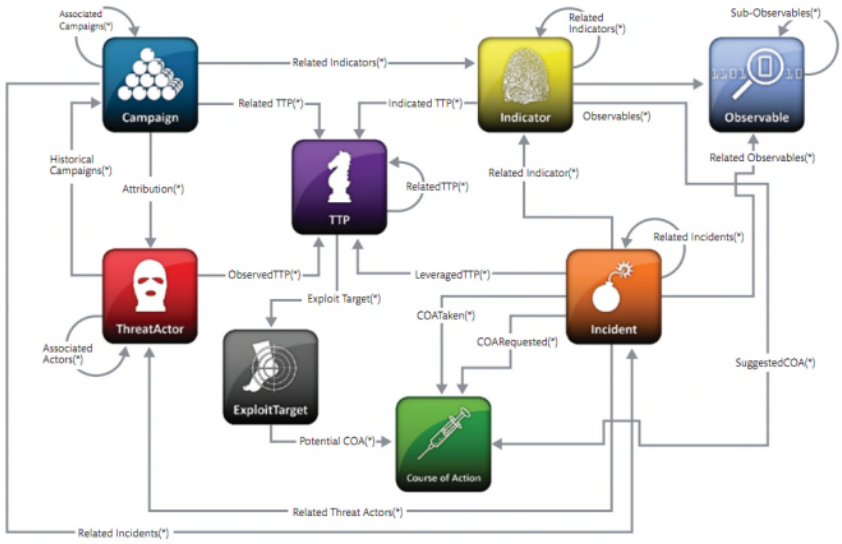
2.1 CybOX

Cyber Observable eXpression (CybOX) adalah skema standar untuk menentukan spesifikasi, pengambilan sampel, karakterisasi, dan komunikasi tentang peristiwa yang diamati dalam wilayah operasional [10]. CybOX digunakan sebagai dasar dalam perangkat lain dari MITRE seperti STIX untuk menjelaskan peristiwa dengan parameter spasial dan temporal [9]. CybOX menawarkan berbagai cara untuk menggambarkan kondisi dan sifat dari aset teknologi informasi yang dapat digunakan untuk melakukan respon insiden, deteksi malware, manajemen insiden, forensik dijital, dan banyak lagi lainnya [11]. Selain itu, CybOX dapat mengungkapkan peristiwa yang akan berlangsung selama serangan dengan probabilitas tertentu, seperti penghapusan file [10].

Gambar 2: Kolaborasi CybOX, STIX, dan TAXII [12]

2.2 STIX

Structured Threat Information Expression (STIX) menggunakan kosakata CybOX dalam pertukan informasi intelijen tentang ancaman yang berkaitan dengan sebuah insiden [9]. STIX adalah bahasa ekspresif, fleksibel, dan extensible berbasis XML yang menyampaikan informasi potensial tentang ancaman *cyber* [10]. STIX dikembangkan secara terbuka dalam forum yang kolaboratif [13]. Data yang dipertukarkan mencakup pengamatan *cyber*, indikator, insiden, TTP (Taktik, Teknik, dan Prosedur) musuh, eksploitasi, tindakan, kampanye tentang serangan *cyber*, dan pelaku ancaman *cyber* seperti yang tergambar pada Gambar 3 . Untuk menggambarkan semua informasi ini, STIX dapat memanfaatkan banyak bahasa berbasis XML lainnya (seperti Snort dan Yara) [10].

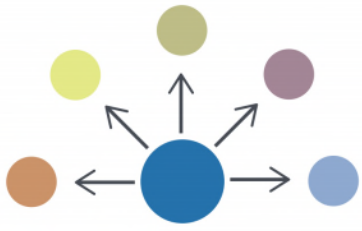


Gambar 3: Arsitektur STIX [13]

2.3 TAXII

Trusted Automated eXchange of Indicator Information (TAXII) merupakan sebuah protokol dan spesifikasi layanan open source yang ditujukan untuk membantu organisasi dalam pertukaran informasi dengan partnernya [9]. Dalam artian lain, TAXII merupakan metoda dalam pertukaran informasi berbasis XML STIX sebagai bahasanya, sehingga memungkinkan proses pertukaran informasi tentang ancaman *cyber* yang terstruktur, aman, dan otomatis [10][14]. Beberpa model pertukaran informasi yang yang didukung adalah sebagai berikut:

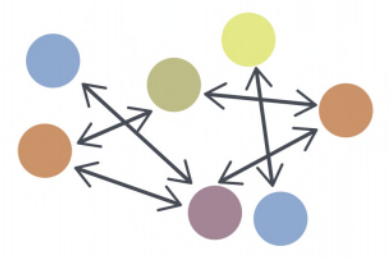
1. **Source/Subscriber,** Sebuah entitas tunggal mempublikasikan informasi kepada sekelompok konsumen. Ini adalah model umum dalam lingkungan komersial, dimana pelanggan membeli akses informasi dari sumber data (vendor) [14].



Gambar 4: Model Source/Subcriber [14]

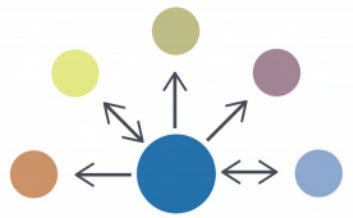
2. **Peer to Peer,** Sekelompok produsen data dan konsumen data yang menjalin hubungan langsung dengan satu sama lain. Kelompok ini mungkin memiliki ke-

bijakan pemerintahan tunggal, tetapi semua pertukaran informasi adalah antara individu-individu [14].



Gambar 5: Model Peer to Peer [14]

3. **Hub and Spoke,** Sekelompok produsen data dan konsumen berbagi informasi satu sama lain, tapi bukan pengiriman langsung. Informasi tersebut dikirim ke hub sentral, yang kemudian hub sentral akan menangani pembagian kepada semua *spoke* yang sesuai. Model ini dapat dikatakan mirip dengan konsep milis [14].



Gambar 6: Model Hub and Spoke [14]

3 Perkembangan Standar

3.1 EU-NIS

Pembentukan platform EU-NIS memiliki tujuan untuk mendorong ketahanan jaringan dan sistem informasi yang dapat mendukung layanan operator pasar dan administrasi publik di Eropa. Pertemuan pertama digelar pada 17 Juni 2013 di Brussels, Belgia. Pembentukan EU-NIS ini juga dimaksudkan untuk menjadi standar implementasi yang bagus pada skala internasional dalam bidang keamanan jaringan dan informasi. Terdapat tiga kelompok kerja:

1. **WG1**: Berfokus pada manajemen resiko, termasuk jaminan informasi, *risk metric* dan peningkatan kewaspadaan;

2. **WG2**: Berfokus pada pertukaran informasi dan koordinasi insiden, termasuk pelaporan insiden dan *risk metric* untuk tujuan pertukaran informasi;

3. **WG3**: Berfokus pada penelitian dan inovasi *Information and Communications Technology* (ICT) yang aman.

Dari ketiga kelompok kerja tersebut, yang paling sesuai dan mencangkup topik makalah ini adalah kelompok kerja kedua (WG2) dimana pertukaran informasi adalah kajian utamanya. Platform NIS diharapkan dapat membantu para pemangku kepentingan untuk melaksanakan manajemen risiko yang tepat, membangun kebijakan keamanan *cyber* yang baik, dan selanjutnya mengadopsi standar dan solusi yang akan meningkatkan kemampuan untuk menciptakan kondisi pasar yang lebih aman bagi Uni Eropa [15].

3.1.1 Ruang Lingkup WG2

Working Group 2 (WG2) bergerak pada segmen organisasi publik maupun privat dalam hal pertukaran informasi di wilayah Uni Eropa. Selain itu semua industri sektor privat juga masuk dalam cakupannya. Fungsi yang dijalankan adalah mengidentifikasi kebutuhan dan rekomendasi isu dalam pertukaan informasi tentang ancaman *cyber* serta proses manajemen insiden yang tepat dalam rangka untuk mencegah dan merespon insiden *cyber* dengan baik. Selain itu, fungsi lainnya mencakup praktek pengamatan saat ini pada penyaluran informasi dan pemberitahuan tentang terjadinya insiden dalam lingkup wilayah Uni Eropa maupun internasional.

Fokus utamanya adalah menjadi sebuah organisasi *Critical National Infrastructure* (CNI) yang bergerak dalam sektor organisasi publik maupun privat yang mapan dalam menangani tata kelola dari ancaman dan insiden yang terjadi. Contohnya pada sektor finansial dimana pertukaran informasi tentang ancaman *cyber* telah terbentuk infrastrukturnya. Selain itu, WG2 dimungkinkan untuk dapat membantu mengembangkan kemampuan *Small and Midsize Business* (SMB) maupun *Small and Midsize Enterprise* (SME) dalam keamanan *cyber* dan bagaimana sektor-sektor tersebut mendapatkan keuntungan dari platform NIS tanpa terlalu dibebani oleh persyaratan wajib. Sedangkan unsur-unsur teknis WG2 melingkupi standar itu sendiri, protokol, dan proses yang tersedia bagi organisasi yang menggunakannya. WG2 juga dapat dilihat dari sudut pandang kewilayahan seperti tingkat nasional hingga benua.

Pada akhirnya WG2 mengakui bahwa privasi dan kepercayaan merupakan pertimbangan utama untuk setiap platform perttukaran informasi. Penangkapan isu, masalah, hingga model kerja yang mungkin didasarkan pada privasi dan kepercayaan dalam pertukaran informasi ancaman *cyber* [15]. Sedangkan topik diskusi beragam utamanya seputar dengan kepercayaan (*trust*) dan hambatan. Dimana kepercayaan dapat diperoleh melalui waktu dan melalui kewajiban kontraktual, sedangkan hambatannya berkenaan dengan teknologi, hukum, dan kebijakan [15].

3.1.2 Tujuan WG2

Terdapat enam tujuan dari WG2, berikut adalah daftar tujuan yang terangkum dalam dokumen [15]:

1. Memahami implikasi dari startegi *EU Cyber Security* dalam WG2;
2. Korelasi dalam praktek pertukaran informasi yang digunakan oleh organisasi publik maupun privat;
3. Memberikan pembinaan dan rekomendasi dalam privasi dan kepercayaan;
4. Usulan kerangka kerja dan standar yang digunakan dalam pertukaran informasi maupun koordinasi insiden;
5. Pendekatan yang berbasis adopsi dalam pertukaran informasi;
6. Mengumpulkan informasi tentang inisiatif serupa di daerah lain untuk pertimbangan dalam interoperabilitas.

Sehingga untuk mendukung tujuan itu semua maka WG2 harus menerbitkan dokumen yang melingkupi: Analisis praktek pertukaran informasi yang digunakan dalam sektor publik dan privat saat ini; Pedoman tentang privasi dan kepercayaan dalam pertukaran informasi; Usulan kerangka kerja dan standar yang akan digunakan untuk pertukaran informasi dan koordinasi insiden, serta pendekatan berbasis adopsi; dan Laporan inisiatif pertukaran informasi di luar daerah WG2.

Dari bahasan pada bagian EU-NIS maka dapat ditarik beberapa kesimpulan sementara secara sederhana tentang *information sharing* berdasarkan sudut pandang EU-NIS sebagai berikut: Belum dirilisnya dokumen sebagai pedoman tentang kerangka kerja dan standar lengkap (masih dalam bentuk *draft*) dalam wilayah kerja WG2; Lingkupnya

adalah multi-nasional dan multi-vendor; Bervariasinya standar pertukaran informasi tiap negara Uni Eropa memunculkan inisiatif penyeragaman standar; Pengembangan dokumen dari WG2 bersifat terbuka yang mengijinkan pendekatan berbasis adopsi sehingga penyeragaman standar secara internasional dapat dimungkinkan terjadi.

3.2 US-NIST

Setelah membahas tentang perkembangan standar EU-NIS, maka selanjutnya akan dibahas tentang perkembangan standar US-NIST yang selanjutnya lebih dikenal dengan istilah NIST saja. NIST merupakan suatu badan yang membuat pengukuran dan menetapkan standar, dan teknologi industri untuk meningkatkan produktivitas, mendukung perdagangan, hingga akhinya mampu memperbaiki kualitas hidup di Amerika Serikat. Dokumen yang berkenaan dengan kerangka kerja (*framework*) cybersecurity diterbitkan awal pada 12 Februari 2014 yang diberi nama "*Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*".

Dokumen tersebut dibuat melalui kerjasama antara industri dan pemerintah, dimana untuk memberikan bimbingan kepada organisasi dalam mengelola resiko dari *cybersecurity*. Sehingga tujuan kestabilan keamanan nasional dan ekonomi Amerika Serikat yang bergantung pada kinerja infrastruktur penting (*critical infrastructure*) dapat terjaga. Untuk memperkuat ketahanan infrastruktur ini, Presiden Obama mengeluarkan *Executive Order* (EO) 13636, dengan judul "*Improving Critical Infrastructure Cybersecurity*" pada 12 Februari 2013 sebagai cikal bakal diterbitkannya dokumen "*Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*". Yang dimaksud infrastruktur penting tersebut adalah organisasi publik maupun privat dari pemilik, pelaku, hingga entitas lain yang memiliki peran dalam mengamankan infrastruktur nasional.

3.2.1 Dasar Kerangka Kerja *Cybersecurity*

Pada dasarnya kerangka kerja tersebut tidak diperuntukkan khusus kebutuhan spesifik dari industri A maupun Negara X. Sebuah organisasi dapat menggunakan kerangka kerja ini sebagai bagian penting dari proses yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko *cybersecurity* [16]. Dengan memanfaatkan kerangka kerja sebagai alat manajemen risiko *cybersecurity*, sebuah organisasi dapat menentukan kegiatan

yang paling penting untuk pemberian layanan kritis dan memprioritaskan pengeluaran untuk memaksimalkan dampak investasi. Sehingga konsep sebagai bahasa umum yang digunakan dalam kerjasama internasional tentang *cybersecurity* pada infrastruktur penting [16] dapat tercapai. Selain itu fungsi lain dari adanya kerangka kerja ini yaitu sebagai cara yang sederhana untuk menyelaraskan percakapan risiko bisnis dan proses teknis dalam operasional.

3.2.2 Kategori dan Fungsi dari Inti Kerangka Kerja

Selaras dengan beberapa persyaratan penting yaitu mengidentifikasi, menilai, dan mengelola risiko *cybersecurity*. Sehingga muncul penetapan fungsi inti dari kerangka kerja adalah sebagai berikut:

1. **Identify,** Mengembangkan pemahaman organisasi untuk mengelola risiko *cybersecurity* untuk sistem, aset, data, dan kemampuan. Sehingga contoh hasil kategori dalam fungsi ini meliputi: *Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.*

2. **Protect,** Mengembangkan dan menerapkan pengamanan yang memadai untuk memastikan distribusi layanan pada infrastruktur penting. Contoh hasil kategori dalam fungsi ini meliputi: *Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.*

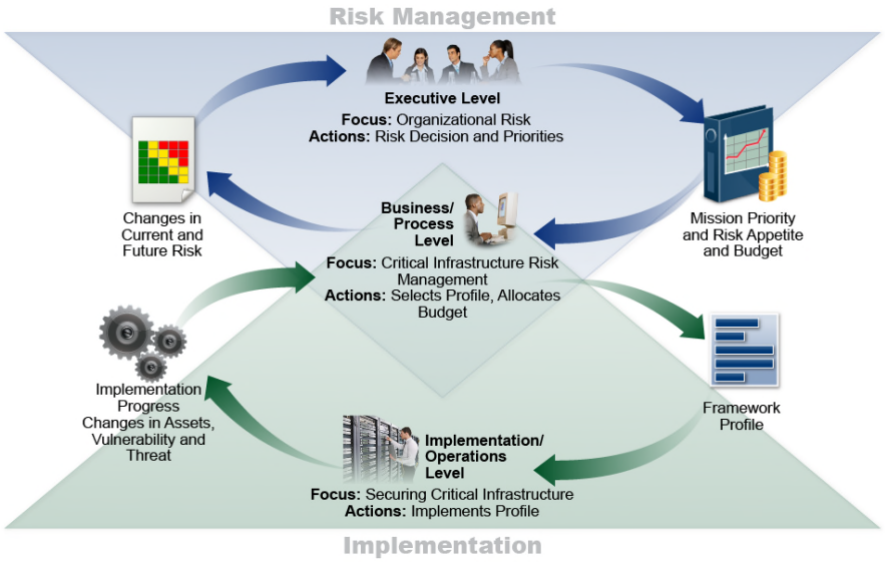
3. **Detect,** Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengidentifikasi terjadinya peristiwa *cybersecurity*. Contoh hasil kategori dalam fungsi ini meliputi: *Anomalies and Events; Security Continuous Monitoring; and Detection Processes.*

4. **Respond,** Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengambil tindakan mengenai peristiwa *cybersecurity* yang terdeteksi. Contoh hasil kategori dalam fungsi ini meliputi: *Response Planning; Communications; Analysis; Mitigation; and Improvements.*

5. **Recover,** Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mempertahankan rencana pertahanan dan mengembalikan setiap kemampuan atau jasa yang terganggu karena peristiwa *cybersecurity*. Contoh hasil kategori dalam fungsi ini meliputi: *Recovery Planning; Improvements; and Communications.*

3.2.3 Implementasi Kerangka Kerja

Konsep pembagaian tingkatan dalam kelas-kelas memberikan konteks tentang bagaimana sebuah organisasi memandang risiko dan proses dari *cybersecurity* untuk mengelola risiko yang mungkin terjadi. Tingkatan tata kelola resiko tersebut terbagi dalam empat tingkatan meliputi: *Partial;Risk Informed; Repeatable;* dan *Adaptive*. Tingkatan-tingkatan tersebut menggambarkan tingkatan kekakuan praktek manajemen risiko *cybersecurity*. Selain itu, untuk mengidentifikasi sejauh mana manajemen risiko *cybersecurity* diinformasikan oleh kebutuhan bisnis dan diintegrasikan secara keseluruhan dalam praktek manajemen resiko sebuah organisasi. Pertimbangan manajemen risiko mencakup banyak aspek *cybersecurity*, termasuk sejauh mana pertimbangan privasi dan kebebasan sipil diintegrasikan dalam manajemen risiko *cybersecurity* dan respon risiko potensial organisasi.



Gambar 7: Arus Keputusan dalam Organisasi [16]

Progresi untuk perubahan tingkat yang lebih tinggi direkomendasikan ketika perubahan tersebut akan mengurangi risiko *cybersecurity* dan mengefektifkan penggunaan biaya. Keberhasilan pelaksanaan kerangka kerja ini didasarkan pada pencapaian hasil yang dijelaskan dalam *target profile* dari organisasi dan bukan pada penentuan kelas tingkatan [16]. Implementasi kerjanya dapat divisualisasikan pada Gambar 7, dimana menggambarkan aliran umum dari informasi dan keputusan dalam beberapa tingkatan umum sebuah organisasi (*Excecutive, Business/Proces,* dan *Implementation/Operations*).

Fungsi dari *target profile* tersebut adalah menyelaraskan standar, pedoman, dan praktek implementasi dari sebuah kerangka kerja yang disusun. Sifat yang terbuka dan mengijinkan untuk saling menyelaraskan atar standar yang lain (ISO, COBIT, ISA, dan CCS) dapat dilihat pada lampiran A pada dokumen [16] yang sekaligus menjadikan nilai tambah dari kerangka kerja yang dirancang ini. Beberapa perusahaan besar (Intel, Boeing, dan FAA) sudah memulai membuat dasar profil risiko keamanan mereka pada kerangka NIST *Cybersecurity* [17].

3.2.4 Publikasi Spesial dan Tantangannya

Information sharing termasuk dalam kelompok keamanan komputer, sehingga publikasi standar yang dikeluarkan NIST tentang pertukaran informasi masuk dalam seri SP 800-XX yaitu SP 800-150. Sama halnya dengan standar EU-NIS, hal spesifik mengenai *information sharing* masih diterbitkan dalam bentuk dokumen rancangan (*draft*). Awal periode perancangan SP 800-150 adalah 29 Oktober 2014 hingga 28 Nopember 2014.

Tidak hanya aktif berkolaborasi dengan industri dan pemerintah, perancangan dokumen SP 800-150 yang sampai saat ini mencapai edisi kedua, juga melibatkan peran dari organisasi akademik [8]. Dokumen tersebut juga merupakan pelengkap dari konsep pendahuluan pertukaran informasi pada bagian keempat dari dokumen SP 800-61 (*Computer Security Incident Handling Guide*)[18].

Beberapa tantangan tentang pertukaran informasi yang dikemukakan dalam dokumen SP 800-150 meliputi: tantangan yang melingkupi dua pihak (pemberi informasi dan penerima informasi); tantangan yang melingkupi pemberi informasi saja; dan tantangan yang hanya melingkupi penerima informasi [8]. Tantangan pertama adalah antara dua pihak meliputi:

1. **Kepercayaan,** pembangunan kepercayaan yang disertai dengan usaha untuk mempertahankan sebuah nilai kepercayaan itu;

2. **Interoperabilitas,** pencapaian interoperabilitas yang membutuhkan standarisasi format data dan protokol dengan cara adopsi, ataupun dengan cara lain yang disepakati;

3. **Perlindungan informasi sensitif,** perlindungan akan informasi yang sensitif (informasi pribadi, kekayaan intelektual, rahasia dagang, atau informasi eksklusif

lainnya yang dapat mengakibatkan kerugian keuangan, pelanggaran perjanjian berbagi, tindakan hukum, dan kehilangan reputasi).

Tantangan kedua adalah yang menyangkut pemberi informasi saja diantaranya:

1. **Patuh akan legalitas hukum dan persyaratan organisasi,** pembatasan jenis informasi mencakup batasan pada jenis informasi dan tingkat detail teknis yang diberikan;

2. **Pembatasan atribut,** dimana organisasi dapat secara terbuka berpartisipasi dalam komunitas pertukaran informasi, hanya saja kontribusi tanpa atribut memungkinkan organisasi untuk dapat berbagi informasi lebih lanjut sambil mengontrol risiko reputasi organisasi;

3. **Aktifasi proses produksi informasi,** dimana organisasi yang ingin menghasilkan informasi harus memiliki infrastruktur, peralatan, dan pelatihan untuk melakukannya, sesuai dengan jenis informasi yang akan diproduksi.

Tantangan terakhir adalah pada sisi penerima informasi diantaranya:

1. **Akses informasi eksternal,** diperlukannya infrastruktur untuk mengakses sumber eksternal dan menggabungkan informasi yang diambil dari sumber eksternal ke dalam proses pengambilan keputusan lokal;

2. **Evaluasi kualitas informasi yang diterima,** validasi data dilakukan sebelum sebuah organisasi mengambil tindakan keamanan yang relevan (seperti konfigurasi ulang perangkat keamanan) berdasarkan informasi yang diterima.

3.3 IETF

IETF merupakan komunitas internasional terbuka yang menjaring berbagai elemen mulai dari *network designer, operators, vendors,* hingga *researchers* yang tertarik dalam perkembangan jaringan dan internet. Selain menjaring pihak organisasional, IETF juga terbuka untuk pihak individual. Misi dari IETF sendiri seperti yang tertuang pada dokumen RFC 3935 [19] dimana membuat internet lebih baik dari sudut pandang teknik melalui penerbitan dokumen yang relevan. Dokumen-dokumen yang dimaksud meliputi: standar protokol; laporan praktek terkini; dan dokumen yang berisi informasi lainnya.

Tidak berbeda jauh dengan EU-NIS dan NIST dimana IETF sendiri membagi topik bahasan ke dalam kelompok kerja yang bersesuaian. Secara mayor, banyak pekerjaan yang ditangani melalui milis. Akan tetapi pertemuan tatap muka tetap diadakan yaitu tiga kali dalam satu tahun. IETF juga merupakan salah pemantik awal dalam praktik standarisasi keamanan dan respon insiden. Hal tersebut tertuang dalam rilis dokumen-dokumen seperti RFC 2196 (*Site Security Handbook*) pada September 1997 [20], RFC 2350 (*Expectations for Computer Security Incident Response*) pada Juni 1998 [21], RFC 3013 (*Recommended Internet Service Provider Security Services and Procedures*) pada Nopember 2000 [22], dan RFC 3227 (*Guidelines for Evidence Collection and Archiving*) pada Februari 2002 [23].

3.3.1 Prinsip Kerja dari IETF

Untuk mendukung tercapainya misi yang sebelumnya dikemukakan, maka IETF menentukan prinsip kerja sebagai berikut [19]:

1. **Open Process,** setiap orang yang tertarik dapat berpartisipasi dalam suatu topik bahasan, mengetahui apa yang sedang diputuskan, dan mengusulkan pandangannya dalam sebuah isu yang terkait;

2. **Technical Competence,** Isu-isu teknis yang dituangkan dalam dokumen IETF merupakan isu kompeten yang dibutuhkan;

3. **Volunteer Core,** partisipasi relawan atau orang-orang yang datang ke IETF karena mereka ingin melakukan pekerjaan secara sukarela untuk mencapai misi IETF;

4. **Rough Consensus and Running Code,** IETF membuat standar berdasarkan penilaian rekayasa gabungan dari peserta dan pengalaman dunia nyata dalam menerapkan dan menggunakan spesifikasi IETF.

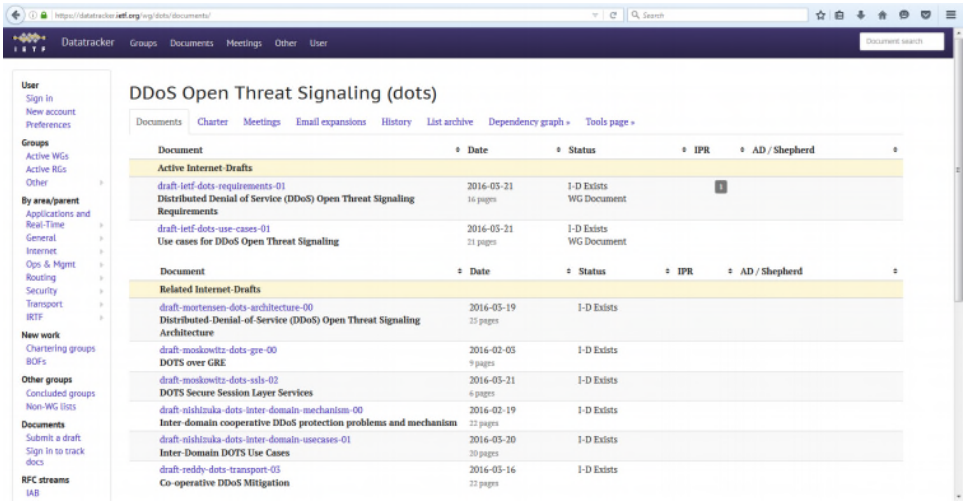
5. **Protocol Ownership,** ketika IETF mengambil kepemilikan sebuah protokol atau fungsi, maka IETF menerima tanggung jawab untuk semua aspek dari protokol, meskipun beberapa aspek mungkin jarang atau tidak pernah dilihat di Internet.

3.3.2 Dokumen Terkait dengan *Information Sharing*

Beberapa hal yang dapat dijadikan rujukan tentang *information sharing* adalah kelompok kerja DOTS (DDoS *Open Threat Signaling*) dan dokumen RFC 5941 (*Sharing Transaction Fraud Data*).

DOTS merupakan kelompok kerja bentukan IETF yang bertujuan untuk mengembangkan standar berbasis pendekatan *realtime signaling* pada DDoS yang berkaitan dengan telemetri dan permintaan penanganan ancaman dan data antara unsur-unsur yang bersangkutan dengan deteksi serangan DDoS, klasifikasi, *traceback*, dan mitigasi. Kelompok kerja ini juga diharapkan mampu menghasilkan satu atau lebih standar spesifikasi yang bekenaan dengan DDoS. Sementara standar yang dihasilakan juga harus dirancang untuk dapat mencakup bahasan aplikasi keamanan jaringan diluar DDoS. Spesifikasi yang dihasilkan mencakup mekanisme standar untuk otentikasi dan otorisasi, integritas data, dan menyediakan privasi dalam operasi yang ramah untuk semua kasus.

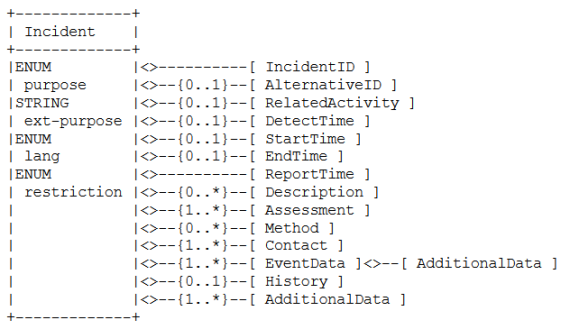
Penerbitan sebuah dokumen yang komprehensif memang membutuhkan waktu yang cukup lama. Kelompok kerja DOTS yang memulai diskusi pada tanggal 12 Februari 2015, hingga saat ini baru menghasilkan dua dokumen rancangan (*draft*) seperti yang terlihat pada Gambar 8 berikut:



Gambar 8: Perkembangan dokumen diskusi DOTS [24]

Dokumen RFC 5941 sudah rilis seacra utuh dan disetujui oleh *Internet Engineeering Steering Group* (IESG), akan tetapi dokumen yang dihasilkan bukan merupakan dokumen yang dapat dijadikan standar internet [25]. Hal tersebut mengacu pernyataan pada dokumen RFC 5741 [26] bahwa tidak semua dokumen yang disetujui oleh IESG

merupakan kandidat dalam tingkatan sebagai standar internet. Dokumen ini menjelaskan format dokumen dalam pertukaran informasi tentang insiden penipuan transaksi dan otentikasi. Informasi ini dimaksudkan untuk digunakan dalam upaya peningkatan efektifitas program deteksi penipuan dan pencegahan. Efektifitas program tersebut sangat bergantung pada keakuratan, kehandalan, kerahasiaan, dan ketepatan waktu dari informasi maupun operator dalam proses pertukarannya. Format data yang digunakan sebagai ilustrasi dalam dokumen RFC 5941 seperti tampak pada Gamabar 9 berikut:



Gambar 9: Model Data dalam beberapa kelas insiden [25]

3.3.3 Upaya Lain dalam *Information Sharing*

Selain kelompok kerja DOTS, IETF sebelumnya juga telah mempelajari otomasi keamanan dan konsep berbagi informasi tentang ancaman dalam beberapa kelompok kerja [10]. Kelompok kerja tersebut meliputi: *Messaging Abuse Reporting Format* (MARF), *Network Endpoint Assessment* (NEA), *Extended Incident Handling* (INCH), *Managed Incident Lightweight Exchange* (MILE), dan *Security Automation and Continuous Monitoring* (SACM).

4 Diskusi

Dalam makalah ini terdapat tiga bahasan utama sebagai solusi dari permasalahan yang menjadi penghambat *information sharing*. Pertama adalah perihal otomasi perangkat, dimana peralihan konsep manual menjadi sebuah fungsi otomasi dapat menggunakan perangkat alternatif yang telah dibahas pada sesi kedua. Kedua adalah inisiatif penyeraman standar, akibat beragamnya jenis standar proses *information sharing* menjadi sebuah penghambat untuk proses itu sendiri. Ketiga adalah peningkatan fungsi interoperabilitas yang memungkinkan implementasi sistem dapat dilakukan dalam wilayah

kerja yang luas. Sehingga secara garis besar tiga pokok bahasan tersebut bersinggungan langsung dengan sektor teknis, kebijakan, dan tata kelola yang saling berkesinambungan.

Sektor teknis menciptakan infrastruktur tangguh guna mendukung terciptanya skema *information sharing* yang otomatis, aman dan terpercaya. Untuk mencapai tujuan tersebut maka akan bersinggungan dengan sektor kebijakan yang memiliki fungsi untuk menciptakan struktur hukum yang tepat tanpa kewajiban hukum yang rumit. Pada akhirnya sebuah kerangka hukum yang disepakati bersama tersebut, diperlukan untuk menciptakan aturan main dalam sektor tata kelola. Hubungan yang sinergi tersebut merupakan solusi dari tujuan otomasi, penyeragaman standar, interoperabilitas antara pemangku kepentingan yang heterogen dan organisasi penyelenggara *information sharing*.

Hingga saat ini belum tercipta sebuah standar *information sharing* tingkat dunia. Adanya inisiatif untuk mengkampanyekan standar berdasarkan kewilayahan seperti US-NIS dan NIST dapat diartikan sebagai dinding penghambat untuk mewujudkan keseragaman standar *information sharing* tingkat dunia. Namun sifat keterbukaaan dari ketiga instansi pengelola standar (EU-NIS, NIST, dan IETF) menjadikan sebuah peluang untuk mengkolaborasikannya, sehingga kemungkinan irisan dalam penyeragaman standar *information sharing* tingkat dunia dapat tercapai. Upaya kolaborasi tersebut pernah dilakukan antara EU-NIS dan US-NIST dalam sebuah pertemuan "*Preliminary Workshop comparing U.S. Cybersecurity framework and EU NIS Platform approaches*" di Brussels pada tanggal 24 Nopember 2014 [27].

4.1 Kolaborasi EU dan US

Terdapat dua panel topik bahasan, yang pertama mengenai paktek manajemen risiko praktek untuk industri. Sedangkan pada panel kedua mengenai inisiatif pembentukan *information sharing* secara sukarela pada tingkat internasional. Pada panel ini dibahas peran dan mekanisme yang mungkin dilaksanakan. Misal keseragaman pandangan dalam menetapkan peran pemerintah sebagai pihak ketiga yang dipercaya dalam pengaturan information sharing. Dalam mekanisme implementasi pada UKM, US mengalami kendala dalam menyelaraskan pengaturan *information sharing* dengan organisasi-organisasi besar. Tetapi EU melaporkan bahwa UKM di Eropa sudah mampu berbagi

informasi menggunakan perangkat dari anti-virus.

Dari pertemuan ini didapat rangkuman bahwa belum ada titik temu satu ukuran yang cocok untuk kedua pihak dalam skala standar. Namun baik EU maupun US menyimpulkan bahwa semua bahasahan dalam pertemuan tersebut bermanfaat untuk dibahas lebih lanjut dan diperhitungkan dengan metoda pendekatan masing-masing [27].

4.2 Pandangan Masa Depan

Dalam sudut pandang positif, dunia akan memiliki banyak pedoman yang komprehensif tentang *information sharing*. Hal tersebut secara langsung meningkatkan nilai kompleksitas pilihan standar alternatif yang akan diterapkan dan berimplikasi juga terhadap kebutuhan dialog fungsional antar standar. Meningkatnya kebutuhan dialog tersebut diakibatkan karena banyaknya pilihan format data dan standar dalam proses mendapatkan standar baru atau penentuan standar yang dianggap lebih komprehensif.

Sehingga untuk langkah berikutnya adalah melanjutkan kolaborasi di wilayah geografis seluruhnya, baik pada sektor teknis, kebijakan, maupun tata kelola. Pembagian kelompok kerja juga dipandang sebagai strategi untuk menyelesaikan masalah teknis secara paralel.

5 Kesimpulan

Keberagaman standar tidak dapat diartikan secara langsung sebagai dinding penghambat dalam *information sharing*. Hal tersebut bergantung dari sisi mana cara memandangnya. Hubungan yang tidak sinergi antara aspek teknis, kebijakan dan tatakelola yang merupakan dinding penghambat dalam *information sharing*, karena tujuan penyelesaian masalah tentang otomasi, penyeragaman standar, dan interoperabilitas tidak dapat dicapai. Menjaga kesinergian antara tiga sector tersebut menjadi sangat penting. Meskipun kepercayaan dapat ditumbuhkan melalui intensitas waktu, akan tetapi kepercayaan juga dapat ditumbuhkan melalui kewajiban kontraktual. Sifat yang terbuka antara EU-NIS, NIST, dan IETF yang memberi peluang upaya kolaborasi dalam penyeragaman standar *information sharing* tingkat dunia dapat tercapai. Segala upaya kolaborasi yang mungkin masih dalam proses pembahasan untuk menciptakan sebuah standar tingkat dunia dengan berbagai pendekatan dan strategi.

Referensi

[1] T. Takahashi and Y. Kadobayashi, "Reference ontology for cybersecurity operational information," *The Computer Journal*, 2014.

[2] T. Takahashi and Y. Kadobayashi, "Cybersecurity information exchange techniques: Cybersecurity information ontology and cybex," *Journal of the National Institute of Information and Communications Technology*, Mar. 2012.

[3] H. Tilawah, "Pertukaran informasi keamanan siber untuk mendukung kolaborasi global," *EL6115-2015: Secure Operation and Incident Handling*, 2015.

[4] C. Zhang and S. Li, "Secure information sharing in internet-based supply chain management systems," *Journal of Computer Information Systems*, vol. 46, no. 4, pp. 18–24, 2006.

[5] Joint Task Force Transformation Initiative, "SP 800-30 rev.1. guide for conducting risk assessments," tech. rep., Gaithersburg, MD, United States, 2012.

[6] N. Adam, A. Kozanoglu, A. Paliwal, and B. Shafiq, "Secure information sharing in a virtual multi-agency team environment," *Electronic Notes in Theoretical Computer Science*, vol. 179, pp. 97 – 109, 2007.

[7] S. Rachuri, E. Subrahmanian, A. Bouras, S. J. Fenves, S. Foufou, and R. D. Sriram, "Information sharing and exchange in the context of product lifecycle management: Role of standards," *Computer-Aided Design*, vol. 40, no. 7, pp. 789 – 800, 2008.

[8] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Second draft SP 800-150. guide to cyber threat information sharing," tech. rep., Gaithersburg, MD, United States, 2016.

[9] D. Rhoades, "Machine actionable indicators of compromise," in *2014 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–5, Oct 2014.

[10] P. Kampanakis, "Security automation and threat information-sharing options," *IEEE Security Privacy*, vol. 12, pp. 42–51, Sept 2014.

[11] MITRE, "Cyber observable expression- a structured language for cyber observables." `https://makingsecuritymeasurable.mitre.org/docs/cybox-intro-handout.pdf`. CybOX intro handout Accessed 5 May 2016.

[12] European Union Agency for Network and Information Security (ENISA), "Detect, share, protect- solutions for improving threat data exchange among certs," tech. rep., Heraklion, Greece, 2013.

[13] MITRE, "Structured threat information expression- structured language for cyber threat intelligence information." `https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf`. STIX intro handout Accessed 5 May 2016.

[14] MITRE, "Trusted automated exchange of indicator information- enabling cyber threat information exchange." `https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf`. TAXII intro handout Accessed 5 May 2016.

[15] W. Grudzien and W. Semple, "WG2 outcome draft - recommendations and guidance for information sharing," tech. rep., Heraklion, Greece, 2013.

[16] National Institute of Standards & Technology (NIST), "Framework for improving critical infrastructure cybersecurity version 1.0," tech. rep., Gaithersburg, MD, United States, 2014.

[17] M. Kaeo, "Global standards unification - how eu nis platform, nist and ietf standards are breaking barriers for information sharing and automated action," in *27th Annual FIRST Conference on Computer Security Incident Handling*, June 2015. Slides of Presentation.

[18] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "SP 800-61 rev.2. computer security incident handling guide," tech. rep., Gaithersburg, MD, United States, 2012.

[19] H. Alvestrand, "A mission statement for the ietf," BCP 95, RFC Editor, October 2004.

[20] B. Fraser, "Site security handbook," FYI 8, RFC Editor, September 1997.

[21] N. Brownlee and E. Guttman, "Expectations for computer security incident response," BCP 21, RFC Editor, June 1998.

[22] T. Killalea, "Recommended internet service provider security services and procedures," BCP 46, RFC Editor, November 2000.

[23] D. Brezinski and T. Killalea, "Guidelines for evidence collection and archiving," BCP 55, RFC Editor, February 2002.

[24] Internet Engineering Task Force (IETF), "DDoS Open Threat Signaling (DOTS)." `https://datatracker.ietf.org/wg/dots/documents/`. Active Internet-Drafts of DOTS Accessed 5 May 2016.

[25] D. M'Raihi, S. Boeyen, M. Grandcolas, and S. Bajaj, "Sharing transaction fraud data," RFC 5941, RFC Editor, August 2010.

[26] L. Daigle and O. K. and, "Rfc streams, headers, and boilerplates," RFC 5741, RFC Editor, December 2009.

[27] European Union Agency for Network and Information Security (ENISA), "Summary report of preliminary workshop comparing u.s. cybersecurity framework and eu nis platform approaches," tech. rep., Brussels, 2014.