BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

DÜNYA ÖRNEKLERİ DOĞRULTUSUNDA TÜRKİYE İÇİN SİBER TEHDİTLERE MÜDAHALE MERKEZİ ÖNERİSİ

Yüksel GÜNAYDIN

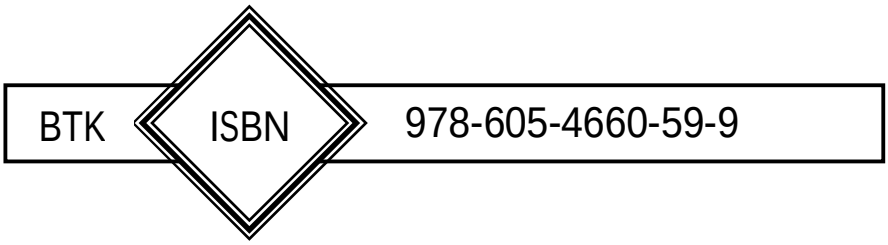
Bilişim Uzmanlığı Tezi

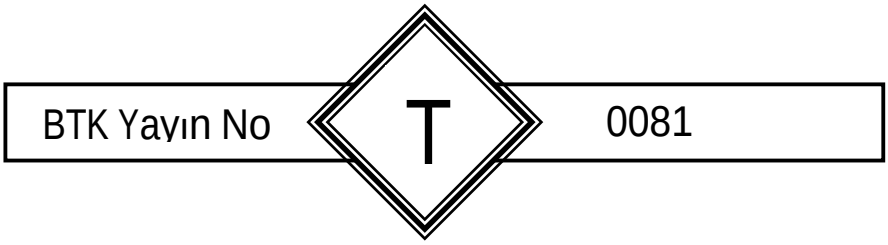
Temmuz 2011

Ankara

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

DÜNYA ÖRNEKLERİ DOĞRULTUSUNDA TÜRKİYE İÇİN SİBER TEHDİTLERE MÜDAHALE MERKEZİ ÖNERİSİ

Yüksel GÜNAYDIN

Bilişim Uzmanlığı Tezi

Temmuz 2011

Ankara

Yüksel GÜNAYDIN tarafından hazırlanan DÜNYA ÖRNEKLERİ DOĞRULTUSUNDA TÜRKİYE İÇİN SİBER TEHDİTLERE MÜDAHALE MERKEZİ ÖNERİSİ adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Ali Aydın SELÇUK
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Kurul Üyesi Galip ZEREY

Üye : Daire Başkanı Mustafa ÜNVER

Üye : Daire Başkanı Osman Nihat ŞEN

Üye : Daire Başkanı Cafer CANBAY

Üye : Bilişim Başuzmanı M. Salim KETEVANLIOĞLU

Üye : Prof. Dr. Haluk GÜMÜŞKAYA

Üye : Yrd. Doç. Dr. Ali Aydın SELÇUK

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Dünya Örnekleri Doğrultusunda Türkiye İçin Siber Tehditlere Müdahale Merkezi Önerisi
Türü	Bilişim Uzmanlığı Tezi
Yazar	Yüksel GÜNAYDIN
Teslim Tarihi	15 Temmuz 2011
Anahtar Kelimeler	Siber tehditler, siber olaylar, koordinasyon merkezi, siber olaylara karşı koyma, Ulusal Siber Tehditlere Müdahale Merkezi
Tez danışmanı	Yrd. Doç. Dr. Ali Aydın SELÇUK
Sayfa Adedi	ix+165

Özet

Ulusal Siber Tehditlere Müdahale Merkezi (U-STİM), siber tehditlerle mücadelede çeşitli hizmetler sunan ve müşterilerine karşı sorumluluğu olan bir yapıdır. U-STİM tek bir koordinasyon merkezi olması dolayısıyla, siber tehditlere ulusal düzeyde müdahalede ve siber olaylara karşı koymada teknik ve hukuki açılardan yararlar sağlamaktadır. Siber tehditlerle etkin bir şekilde mücadele edilebilmesi için, konu ile ilgili tüm tarafların işbirliği içerisinde çalışması ve bu alanda ülkemizin yoksun kaldığı hukuki düzenlemelerin yapılması önem arz etmektedir. Bu çalışmada siber tehditleri sınıflandırma yaklaşımları ve U-STİM yapısı hakkında genel bilgiler verilmiş, U-STİM tarafından sunulan hizmetler incelenmiş, konuya ilişkin uluslararası platformlar ve dünya uygulamaları gözden geçirilmiş, siber tehditlere müdahale konusunda ülkemizdeki mevcut durum ele alınmış ve U-STİM yapısının kurulması konusunda öneriler sunulmuştur.

ABSTRACT

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY	
Thesis	Cyber Threats Response Center Proposal For Turkey In Accordance With World Examples
Type	ICT Expert Thesis
Author	Yüksel GÜNAYDIN
Submission Date	July 15, 2011
Key Words	Cyber Threats, Cyber Incidents, Coordination Center, Incident Response, National Cyber Threat Response Center
Advisor	Assistant Professor Ali Aydın SELÇUK
Total Page	ix+165

Abstract

National Computer Emergency Response Team (N-CERT) is a center that offers variety of services to combat cyber threats and who has responsibilities towrads its constituency. Due to it provides a single coordination center, N-CERT provides technical and legal benefits while responding to cyber threats and cyber incidents at national level. In order to effectively combat cyber threats, working with all relevant stakeholders in cooperation and making legal regulations is of great importance. In this study, approaches to classify cyber threats is examined and general information about the sturcture of N-CERT is given, services offered by N-CERT are examined, international platforms and world examples on the issue are revised, current situation in our country about responding to cyber threats is dealed and recommendations are presented for establishing a N-CERT.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Yrd. Doç. Dr. Sn. Ali Aydın SELÇUK'a, yine kıymetli tecrübelerinden faydalandığım Bilgi Teknolojileri Dairesi Başkanı Sn. Mustafa ÜNVER'e, Bilişim Uzmanları M. Salim KETEVANLIOĞLU, K. Sacid SARIKAYA ve Demet KABASAKAL'a, konu ile ilgili değerli bilgilerini benimle paylaşan Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Bilişim Suçlarıyla Mücadele Şube Müdürü Emniyet Amiri Bilal ŞEN'e, Bilişim Uzman Yardımcısı Hüseyin Burhan ÖZKAN'a, tüm çalışma arkadaşlarıma ve aileme gönülden teşekkür ederim. Kızım Sinem Elif'e sevgilerimi sunarım.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

(ISC)²	Information Systems Security Certification Consortium, Inc. Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu
AB	Avarupa Birliği
ABD	Amerika Birleşik Devletleri
ADA	Avrupa Dijital Ajandası
AK	Avrupa Konseyi
APCERT	Asia-Pasific CERT Asya-Pasifik STİM
APSIRC	Asia-Pacific Security Incident Response Coordination Asya-Pasifik Güvenlik Olaylarına Müdahale Koordinasyonu
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
ISF	Information Security Forum Bilgi Güvenliği Forumu
CCC	Cyber Clean Center Siber Temizlik Merkezi
CERT	Computer Emergency Response Team Bilgisayar Olaylarına Müdahale Ekibi
CERT/CC	CERT/Coordination Centre STİM Koordinasyon Merkezi
CIAC	Computer Incident Advisory Capability Bilgisayar Olayları Danışma Birimi
CloudCERT	BulutSTİM
CNCERT/CC	China CERT/Coordination Centre Çin U-STİM/KM'si
CSA	Cloud Security Alliance Bulut Güvenlik Birliği
CSIRT	Computer Security Incident Response Team Bilgisayar Güvenlik Olaylarına Müdahale Ekibi
CTO	Commonwealth Telecommunications Organisation

	İngiliz Uluslar Örgütü Telekomünikasyon Birliği
DHS	Department of Homeland Security
	İç Güvenlik Bakanlığı
DNS	Domain Name System
	Alan adı sistemi
DoS	Denial of Service
	Hizmeti durdurma
DPT	Devlet Planlama Müsteşarlığı Teşkilatı
EC-Council	The International Council of Electronic Commerce Consultants
	Uluslararası Elektronik Ticaret Danışmanları Konseyi
EGC	European Government CSIRTs
	Avrupa Kamu-STİM'leri
EGM	Emniyet Genel Müdürlüğü
EHK	Elektronik Haberleşme Kanunu
ENISA	European Network and Information Security Agency
	Avrupa Ağ ve Bilgi Güvenliği Ajansı
ESCAPE	Electronically Secure Collaborative Application Platform for Experts
	Uzmanlar için elektronik güvenli işbirliği platformu
EuroCERT	European CERTs
	Avrupa STİM'leri
FIRST	Forum of Incident Response and Security Teams
	Olaylara Müdahale ve Güvenlik Ekipleri Forumu
GAM	Güvenlik Alarm Merkezi
GCA	Global Cybersecurity Agenda
	Küresel Siber Güvenlik Ajandası
GRC	Global Response Center
	Küresel müdahale merkezi
I4	International Information Integrity Institute
	Uluslararası Bilgi Bütünlüğü Enstitüsü
IGSS	IMPACT Government Security Scorecard
	IMPACT Devlet Güvenlik Puan Kartı

IMPACT	International Multilateral Partnership Against Cyber Threats Siber tehditlere karşı uluslararası çok taraflı ortaklık
IP	Internet Protocol İnternet protokolü
IRON	IMPACT Research Online Network IMPACT Çevrimiçi araştırma ağı
ISACs	Information Sharing and Analysis Centers Bilgi Paylaşımı ve Analiz Merkezleri
ISO	International Organization For Standardization Uluslararası Standardizasyon Örgütü
ITU	International Telecommunication Union Uluslararası Telekomünikasyoın Birliği
IWWN	International Watch and Warning Network Uluslararası İzleme ve Uyarma Ağı
İSS	İnternet Servis Sağlayıcı
JPCERT/CC	Japan CERT/CC Japonya U-STİM/KM
Kamu-STİM	Govermental CSIRT Kamu STİM'i
KBA	Köle Bilgisayar Ağı
KMS	Kısa Mesaj Servisi
KOM	Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı
K-STİM	Koordine STİM
KYMP	Kötücül Yazılımlarla Mücadele Projesi
NCSD	National Cyber Security Division Ulusal Siber Güvenlik Birimi
NEWS	Network Early Warning System Ağ Erken Uyarı Sistemi
NIST	National Institute of Standards and Technology Ulusal Standartlar ve Teknoloji Enstitüsü
NM-SIG	Network Monitoring Special Interest Group Ağ İzleme Özel İlgi Grubu

OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation Operasyonel Olarak Kritik Tehdit, Varlık ve Açıklıkların Değerlendirilmesi
OLTA	Olay Takipçisi
PGP	Pretty Good Privacy Çok iyi gizlilik
RFC	Request For Comment Yorum talebi
RFID	Radio-Frequency Identification Radyo Frekansı İle Tanımlama
S/MIME	Secure/Multipurpose Internet Mail Extensions Güvenli / Çok Amaçlı Elektronik Posta Uzantıları
SANS	SysAdmin, Audit, Network, Security Sistem yöneticisi, Denetim, Ağ ve Güvenlik
SIRCE	Security Incident Response Coordination for Europe Avrupa İçin Güvenlik Olaylarına Müdahale Koordinasyonu
SLA	Servis Seviyesi Anlaşması
SQL	Structured Query Language Yapısal sorgu dili
SSL	Secure Sockets Layer Güvenli yuva katmanı
STİM	Siber Tehditlere Müdahale Merkezi
TBMM	Türkiye Büyük Millet Meclisi
TCP	Transmission Control Protocol İletim Kontrol Protokolü
TERENA	Trans-European Research and Education Networking Association Trans-Avrupa Araştırma ve Eğitim Ağı Birliği
TF-CSIRT	Task Force CSIRT Görev Gücü STİM
TR-BOME	Türkiye Bilgisayar Olaylarına Müdahale Ekibi

TR-BOME KM	TR-BOME Koordinasyon Merkezi
TÜBİTAK	Türkiye Bilimsel ve Akademik Araştırma Kurumu
TÜİK	Türkiye İstatistik Kurumu
UDP	User Datagram Protocol
	Kullanıcı Datagram Protokolü
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
ULAKNET	Ulusal Akademik Ağ
USGT	Ulusal Siber Güvenlik Tatbikatı
USGS	Ulusal Siber Güvenlik Stratejisi
US-CERT	United State CERT
	ABD U-STİM
UST@M	Ulusal STİM
U-STİM	Ulusal STİM
WARPs	Warning and Alerting Points
	Uyarı ve Alarm Noktaları
WCSS	World Cyber Security Summit
	Dünya Siber Güvenlik Zirvesi

GİRİŞ

Bilgi ve iletişim teknolojileri (BİT) ekonomik ve sosyal gelişmenin temel faktörü haline gelmiştir. Artık bilgisayara ve internete elektrik ve su gibi hemen her yerde ulaşmak mümkündür. Kişilerin ekonomik ve sosyal hayatını kolaylaştıran ve dünya üzerindeki farklı coğrafyalarda yaşayan kullanıcıların etkileşime geçmelerine olanak sağlayan BİT'lerin kullanımı ülkemizde de önemli oranda artmaktadır. Türkiye İstatistik Kurumu (TÜİK) verileri, ülkemizde 2011 yılı itibariyle hanelerin % 42.9'unun internet erişim imkânına sahip olduğunu, 16-74 yaş grubu bireylerin %45.0'nin internet kullandığını göstermektedir.

BİT'lerin yaygınlık kazanması tüketicilere ve işletmelere birçok faydalar sunduğu gibi organize suçlar için de bir zemin oluşturmaktadır. Doğası gereği küresel bir ortam sunan internet, her türden kullanıcıya ve işletmeye bu ortamda para kazanma ve her türden bilgiye ulaşma olanağı sunmaktadır. Sanal dünyaya ve sanal ekonomiye ev sahipliği yapan internet, bu özelliği ile suçlular da dâhil olmak üzere birçok insanın ilgisini çekmektedir. Bu durum, gerçek dünyada işlenen kadar suçun, fiziksel ortamda var olan kadar tehdidin sanal ortamda kullanıcıları hedef alması sonucunu doğurmaktadır. Bir güvenlik araştırma firması olan Sophos, 2011 yılının ilk yarısında her 4.5 saniyede bir internet tehdidinin ortaya çıktığını, günlük tespit edilen kötücül yazılım örnek sayısının 150.000 olduğunu, ifade etmektedir. Stuxnet gibi endüstriyel kontrol sistemlerindeki güvenlik açıklıklarını kullanan ve ülkelerin kritik altyapılarını hedef alan kötücül yazılımların ortaya çıkması ile birlikte, ülkemizdeki kritik altyapıların da büyük tehdit altında olduğunu söylemek mümkündür.

İnternetin kullanılması ile birlikte hedefli ağ saldırılarında artış görülmeye başlamıştır. Örneğin Türkiye'de uygulamaya konulması planlanan güvenli internet projesini engellemek üzere, kendilerini uluslararası bilgisayar aktivistleri olarak tanıtan Anonymous tarafından 9 Haziran 2011 tarihinde Telekomünikasyon İletişim Başkanlığı'nın (TİB) sistemlerine 100 bin köle bilgisayar ile saldırı

gerçekleştirilmiştir. Söz konusu saldırıya ülke dışından ve ülke içinden binlerce köle bilgisayar katılmıştır.

Siber ortamda kullanıcıları ve sistemleri en çok, genellikle kullanıcısının haberi olmadan bilgisayara bulaşan, o bilgisayarı köle bilgisayar yapan ve bir köle bilgisayar ağına (KBA) dâhil eden kötücül yazılımlar tehdit etmektedir. Microsoft verilerine göre, ülkemizde 2009 yılının son iki çeyreğinde ve 2010 yılının ilk çeyreğinde bu tür kötücül yazılımların bulaşma oranları dünya ortalamasının üstünde olmuştur.

Ülkemizde kötücül faaliyetlerdeki artış, siber ortamdaki kullanıcıların birçok siber tehditle karşı karşıya kalmasına yol açmaktadır. Güvenlik firması AVG, Türkiye'de 2010 yılında her on kullanıcıdan birinin bir siber tehdide maruz kaldığı, dolayısıyla ülkemizin internete bağlanmak için en riskli ülkeler sıralamasında ilk sırada yer aldığı bilgisine yer vermektedir. Bundan başka Microsoft, 2010 yılının ilk çeyreğinde SQL enjeksiyonu saldırılarının hedefleri arasında ".tr" uzantılı alan adına sahip internet sayfalarının ilk sırada yer aldığını ifade etmektedir.

Artan siber tehditlere ve saldırılara karşı, ülkemizin siber güvenlik konusundaki kapasitesinin ve her seviyedeki özellikle de yönetici seviyesindeki farkındalığın arttırılması amacıyla 25-28 Şubat 2011 tarihleri arasında bir siber güvenlik tatbikatı gerçekleştirilmiştir. Tatbikata 41 kurum ve kuruluş katılım sağlamıştır. Çalışmanın sonucunda yapılan tespitlere bakıldığında, bilgi güvenliği yönetim sistemi, siber güvenlik konusunda teknik uzmanlık düzeyi, insan faktörü ve sosyal mühendislik saldırıları, kurum içi ve kurumlar arası koordinasyon, kablosuz ağların güvenliği ve kurumsal internet sayfalarının güvenliği konularında ciddi eksikliklerimizin olduğu görülmektedir.

Küresel bir sorun olan siber tehditlerin saldırıya dönüşmesi ve bir organizasyonu hedef alması durumunda, olaya hızlı ve etkin bir şekilde yanıt vermek söz konusu organizasyon için büyük önem arz etmektedir. Bu ihtiyacı karşılamak, siber tehditlerle ve siber olaylarla mücadele edecek resmi bir yapının kurulması ile

mümkündür. Bununla birlikte, sınır aşan bir yapıya sahip olan siber tehditlerle ve siber olaylarla mücadele ancak uluslararası işbirliği ile yürütüldüğünde etkin ve verimli olabilmektedir. Zira siber olayları gerçekleştirenler, olayın hedefi ve olayı kontrol eden sistemler birbirinden farklı coğrafyalarda bulunabilmektedir. Böyle bir durumda uluslararası işbirliği olmaksızın siber olayın başarılı bir şekilde bertaraf edilmesi ve olayı gerçekleştirenlerin belirlenmesi mümkün olmamaktadır. Bu gerçekten hareketle Avrupa Komisyonu, 2020 yılını hedef alan Avrupa Dijital Ajandası'nı (ADA) oluşturmuştur. Söz konusu Ajanda, 2012 yılı sonu itibariyle, Avrupa Birliği üyesi ülkelerin **U**lusal **S**iber **T**ehdi**t**lere Müdahale **M**erkezlerini (U-STİM) kurmaları ve bu U-STİM yapılarının birbirleri ile işbirliği içinde çalışabilecekleri bir ağın kurulması planlanmaktadır.

Siber tehdidin global düzeyde ciddi boyutlara ulaşmasından ve bu tehdidin ülkemizin güvenliğine etkilerinden hareketle, siber tehditlerin engellenmesine yönelik ulusal düzeyde çalışmalar yapılması ihtiyacını doğurmaktadır. Bu bağlamda siber tehdit konusunun Milli Güvenlik Siyaset Belgesi'ne girdiği bilinmektedir.

Bu tez çalışmasında BİT'leri hedef alan siber tehditlerin neler olduğu, bu tehditlerle mücadelede önemli bir yapı olan ve çoğunlukla Bilgisayar Olaylarına Müdahale Ekibi (BOME, Computer Emergency Response Team - CERT) veya Bilgisayar Güvenlik Olaylarına Müdahale ekibi (BGOME, Computer Security Incident Response Team - CSIRT) olarak ifade edilen, bu çalışma boyunca ise **S**iber **T**ehdi**t**lere Müdahale **M**erkezi (STİM) olarak adlandırılan birimlerin ulusal bir merkez olarak yapısına, sunması gerektiği hizmetlere, bu yapıların siber tehditleri ve siber olayları ele alma ve bertaraf etme yöntemlerine, dünyadaki diğer STİM'ler ile kurulmasında yarar görülen işbirliği çeşitlerine, diğer ülkelerin uygulamalarına, siber tehditlere ve siber olaylara ilişkin dünyadaki işbirliği platformlarına, Türkiye'nin STİM konusunda mevcut durumuna ilişkin bilgiler verilmekte ve ülkemizde konu ile ilgili yapılması gerekenler hakkında öneriler sunulmaktadır.

Çalışmanın birinci bölümünde; BİT'lerin özellikle de internetin, son yıllarda baş döndürücü bir hızla gelişmesine ve tüm dünya çapında yayılmasına paralel olarak

artış gösteren siber tehditlerin neler olduğuna, nasıl sınıflandırıldığına ve STİM'e ilişkin genel bilgiler verilmektedir. İkinci bölümde; siber ortamdaki tehdit ve saldırılarla mücadele edilmesinde ve bu saldırıların yol açtığı zararların bertaraf edilmesinde kullanılan en önemli araç olan STİM altyapısının geliştirilmesi, bu yapının müşterilerine sunabileceği hizmetler, siber tehditlerin ve siber olayların bu yapı tarafından ele alınması, STİM'ler tarafından kurulabilecek işbirlikleri anlatılmaktadır. Üçüncü bölümde STİM konusundaki dünya uygulamaları, dördüncü bölümde ise uluslararası işbirliği platformları incelenmektedir. Beşinci bölümde ülkemizin STİM konusundaki mevcut durumu ele alınmakta ve konu ile ilgili yapılabileceklere ilişkin öneriler anlatılmaktadır.

1. SİBER TEHDİTLER VE U-STİM ALTYAPISI

Yaygın bir kullanım oranına sahip olan BİT'ler her geçen gün gelişmekte ancak bu teknolojilerin yapısı daha da karmaşık hale gelmektedir. Hem yaygın olan hem de birçok kişinin kullanmakta zorluk yaşadığı bu teknolojiler nedeniyle, kullanıcı hatalarından kaynaklanan güvenlik açıkları oluşmakta ve kullanıcılar çok sayıda siber tehdidin hedefi haline gelmektedir. Bu bölümde siber tehditleri sınıflandırma yaklaşımları ele alınmakta ve bu tehditlere müdahale edecek yapılardan bahsedilmektedir.

Siber suçların dünya üzerinde yıllık ne kadar bir kayba yol açtığı net olarak bilinmemektedir. Zira bilgisayar suçlarının çok azının raporlandığına inanılmaktadır. Ekonomik kaygılar nedeniyle birçok şirketin, hisse senetleri üzerinde oluşabilecek olumsuz etkiden korktukları için meydana gelen siber olayları ve kendi sistemlerine yapılan saldırıların detaylarını gizleme eğiliminde olduğu düşünülmektedir. Dolayısıyla siber suçluların elde ettikleri başarıları gizlemekten ziyade duyurma eğiliminde olması ya da bu konuda herhangi bir kaygılarının olmaması, siber saldırıdan etkilenen kişilerin veya organizasyonların bu durumu ilgili birimlere raporlamaktan çekinmeleri, raporlanan olayların buzdağının sadece görünen kısmı olduğu gerçeğini gün yüzüne çıkarmaktadır (Gelbstein ve Kamal, 2002). Bu durumdan hareketle daha çok ve daha karmaşık siber saldırının gerçekleştirilmesi için siber saldırganların oldukça elverişli bir ortama sahip oldukları sonucunu çıkarmak mümkündür.

Siber saldırılarda bir tek saldırgan tarafından gerçekleştirilen saldırıların gerçek tehlikeyi oluşturmadığı, asıl tehlikeyi genç kullanıcıların yeteneklerinin sömürüldüğü ve suça kanalize edildiği organize siber saldırıların ve siber terörizmin oluşturduğu ifade edilmektedir (Gelbstein ve Kamal, 2002).

1.1.Siber Tehditleri Sınıflandırma Yaklaşımları

Siber tehditlerle mücadele edilebilmesi amacıyla tehditler çeşitli sınıflandırmalara tabi tutulmaktadır. Böylece tehditlerin saldırıya dönüşmelerine fırsat verilmeden her

kategorideki her bir tehdit için alınması gereken güvenlik önlemlerinin sistematik bir şekilde belirlenebilmesi imkânı oluşmaktadır

Geleceği tahmin etmenin zorluğu hemen herkesin kabul ettiği bir gerçektir. BİT altyapılarını gelecekte tehdit edecek saldırıların önceden belirlenmesinin de aslında oldukça zor bir çalışma olduğunu söylemek mümkündür. Toplumsal ve ekonomik hayattan bağımsız olması düşünülemeyen BİT'lerin haberleşmeyi, üretimi, ulaşımı ve ticareti kolaylaştıran bir platform haline geldiği günümüzde BİT'lere yönelik siber tehditler, insanların hayatını ciddi bir şekilde etkileyecek ve bu tehditlere karşı yeterli korumanının sağlanması gerekecektir (Gelbstein ve Kamal, 2002).

Gelecekte ortaya çıkması muhtemel sorunların tespit edilmesi ve beklenen tehditlere karşı bir mücadele ve savunma stratejisinin geliştirilmesi mümkün görülmektedir. Bu stratejilerle, siber tehditler mücadele edilmesi zor boyutlara ulaşmadan çözüm adımlarının hazırlanması mümkündür (Gelbstein ve Kamal, 2002). IBM firması etkili bir siber savunmanın ancak, tehdidin tespit edilmesi, analiz edilmesi, sınıflandırılması ve anlaşılması ile mümkün olabileceğini düşünmektedir (IBM, 2010).

Siber tehditlerin tamamen anlaşılmadan yeteri kadar bertaraf edilemeyeceği Georgia Tech Üniversitesi Bilgi Güvenliğ Merkezi (Georgia Tech Information Security Center - GTISC) tarafından da dile getirilmektedir. Siber saldırganları motive eden nedenlerin ve siber saldırganların kullandıkları metotların araştırılması, analiz edilmesi, anlaşılması ve bu bilgilerin geniş kitlelerle paylaşılması tehditlerin anlaşılmasına yönelik çabalar olarak gösterilmektedir (GTISC, 2011).

Ayrıca, birçok siber tehdidin teknik yetenekleri ve amaçları hakkında yeterli bilgiye sahip olunmadığı gözlemlenmiştir. Zira siber tehditlerin, hasar vermek, siyasi veya finansal kazanç elde etmek veya siber suçlulara şöhret getirmek gibi farklı hedefleri olabilmekte ve bu hedefleri gerçekleştirmede kullandıkları çok çeşitli ve sayıda yetenekleri bulunabilmektedir. Tehditlerin ve açıklıkların söz konusu yeteneklerinin,

amaçlarının ve geleceğe ilişkin eğilimlerinin belirlenebilmesi için de siber tehditlerin kapsamlı bir analize tabi tutulması gerektiği belirtilmektedir (Masera vd., 2011).

GTISC yöneticilerinden Mustaque Ahamad'ın aşağıda yer alan görüşlerine bakıldığında, siber tehditlerle mücadelede ve tehditlerin incelenmesi aşamalarında her alandan uzmanın işbirliği içinde çalışması gerekmektedir.

> Fiziksel sistemlerin daha çok bilgiye dayalı hale gelmesiyle, diğer alanlarda gördüğümüz saldırı türleri bu alanda da görülecektir. Bu durum, siber tehditlerin tamamen anlaşılması ve önlenmesi için sadece teknik uzmanların değil, geniş yelpazedeki alanlardan uzmanların işbirliğini gerektiren bir endişedir (GTISC, 2011).

Siber tehdidin üzerinde mutabık kalınmış bir tanımı olmamakla birlikte çözüm önerilerinin geliştirilmesine katkı sağlayacağı düşünülerek çeşitli tanımlar yapılmaktadır. Tehdidin kaynağına, kullandığı teknik ve teknolojilere ve şekline göre (uzaktan, ağ üzerinden, uygulama ile gibi) tanımlamalar yapılabilmektedir (IBM, 2010).

Bir riskin azaltılması, istenmeyen durumların kapsamlı bir şekilde değerlendirilmesine ve sınıflandırılmasına bağlıdır. Tehditle mücadele ancak bu değerlendirme ve sınıflandırma çalışmasından sonra yapılabilmektedir. Riskin veya tehdidin kaynağının ve etkisinin belirlenmesi siber savunmada önem arz etmektedir (IBM, 2010).

Siber tehditlerin sınıflandırılması için çeşitli çalışmalar yapılmıştır. Özellikle akademisyenlerin ve BİT sektöründeki uzmanların katıldığı FORWARD[1] projesi bu çalışmalar arasında yer almaktadır. Proje ile gelecekte ortaya çıkması muhtemel tehditlerin tespit edilmesi amacıyla üç çalışma grubunun kurulduğu, gruplardan birinin kötücül yazılımlar ve dolandırıcılıkla ilgili tehditler üzerinde, diğer bir grubun gelişen akıllı ortamlarla ilgili, bir diğer grubun ise kritik sistemlere ilişkin çalışmalar yürüttükleri ifade edilmektedir. Geleceğin tehditlerinin sistematik bir şekilde ortaya

[1] FORWARD, BİT'lerin korunması amacıyla akademik dünya ile sektör arasında işbirliğini teşvik eden bir Avrupa Komisyonu girişimidir.

koyulması amacıyla söz konusu grupların çalışmalarına yön verecek dört ana eksen belirlenmiştir. Bu eksenler yeni teknolojiler, yeni uygulamalar, yeni iş modelleri ve sosyal dinamikler olarak belirlenmiştir. Proje çalışmalarının sonucu olarak sekiz kategoride 28 adet tehdit tespit edilmiştir (Tablo 1.1) (FORWARD, 2010).

Tablo 1.1. Tehdit kategorileri ve tehditler

No	Tehdit Kategorisi	Tehdit
1	Ağ (A)	Yönlendirme altyapısı
		IPv6 ve bilgisayarların doğrudan erişebilirliği
		Adlandırma (Alan adı sistemi, Domain Name System - DNS) ve kayıt kurumları
		Kablosuz haberleşme
		Hizmeti engelleme
2	Donanım ve sanallaştırma (D&S)	Kötücül donanım
		Sanallaştırma ve bulut bilişim
3	Zayıf cihazlar (ZC)	Sensörler ve Radyo Frekansı İle Tanımlama (Radio-frequency identification - RFID)
		Mobil cihaz kötücül yazılımları
4	Karmaşıklık (K)	Beklenmedik ard arda etkiler
		Ölçeğe ilişkin tehditler
		Sistemin bakım kolaylığı ve doğrulanabilirliği
		Gizli işlevsellik
		Paralelliğe ilişkin tehditler
5	Veri tahrifatı (VT)	Gizlilik ve yaygın sensörler
		Yanlış sensör verileri
		Sosyal ağa ilişkin tehditler
		Çevrimiçi oyunlar
6	Saldırı altyapısı (SA)	Yer altı ekonomisi destek yapıları
		Gelişmiş kötücül yazılımlar
7	İnsan faktörü (İF)	Kullanıcı arabirimi
		İçeriden gelen tehditler
		Emniyetin güvenlikten öncelikli olması
		Mağdurlara ulaşmak için yeni vektörler
		Hedefli saldırılar ve yemlemeler
8	Yetersiz güvenlik gereksinimleri (YGG)	Eski sistemlerin güvenliğinin güçlendirilmesi
		Ticari bileşenlerin kullanılması
		Yeni nesil ağlar

Kaynak: FORWARD, 2010

i. **Ağ:** Bu kategori yeni ağ teknolojilerinin tanıtımına ve uygulanmasına ilişkin tehditleri kapsamaktadır. Ayrıca mevcut durumda altyapı hizmetlerini hedef alan tehditler de bu başlık altında değerlendirilmektedir.

ii. **Donanım ve sanallaştırma:** Bu başlıkta işlemlerin sanal bilgisayarlara ya da bulut sistemlere taşınmasına imkân sağlayan donanım ve yazılımlara ilişkin tehditler incelenmektedir. Kötücül donanımlar da yine donanım ve sanallaştırma kapsamındaki tehditler arasında yer almaktadır.

iii. **Zayıf cihazlar:** Hem hesaplama hem de güç kısıtlamalarından dolayı sınırlı olan yeni BİT cihazları ile ortaya çıkan tehditler bu kapsama girmektedir. Bu durumda, hem gerekli güvenliğin sağlanması işleminin pahalı olması hem de bu cihazların gerekli güvenlik mekanizmalarının uygulanması için yetersiz kalması söz konusu olabilmektedir.

iv. **Karmaşıklık:** Gelecekteki sistemlerin milyarlarca bileşenden oluşma ihtimali ile ortaya çıkan tehditler bu başlık altında ele alınmaktadır. Karmaşıklığın bir nedeni olarak tek parça halindeki sistemler (monolitik sistemler) gösterilmektedir. Karmaşıklığın artması beklenmeyen ve istenmeyen bağımlılıklara, etkileşimlere ve güvenlik sorunlarına yol açabilmektedir.

v. **Veri tahrifatı:** Kullanıcıların ve sistemlerin giderek çok daha fazla miktardaki değerli ve hassas verileri çevrim içi ortamlarda saklaması verilerin tahrif edilmesine ilişkin tehditleri ortaya çıkarmaktadır.

vi. **Saldırıların altyapıları:** Saldırganların aktif bir şekilde KBA gibi saldırı platformları oluşturmaları ve bunları kullanmaları saldırı altyapılarına ilişkin tehditleri ortaya çıkarmaktadır. Siber saldırganlar artık vur-kaç saldırıları düzenlemek yerine kötücül kampanyalar yürütmek için internette operasyonel üsler kurmaktadırlar.

vii. **İnsan faktörü:** İnsan faktörü siber güvenlikte önemli bir rol oynamaktadır. Bu kategoriye giren tehditler kapsamında, özellikle dışarıdan hizmet satın alınması durumlarında içeriden yapılabilecek saldırılar yer almaktadır. Yeni sosyal mühendislik saldırılarına ilişkin tehditler de bu kapsamda incelenmektedir.

viii. **Yetersiz güvenlik gereksinimleri:** Eski ve yeni ticari BİT ürünlerinin yeterli korumaya sahip olarak geliştirilmemesinden kaynaklanan sorunlar ve tehditler bu kapsamda incelenmektedir.

Tehditlerin kategorilere ayrılması çalışmasından sonra söz konusu 28 tehdidin her biri ile mücadele edilmesi amacıyla önceliklendirme çalışmaları yapılmıştır. Önceliklendirmede aşağıda sıralanan dört faktörün dikkate alındığı görülmektedir:

- **Etki:** Bu faktör, söz konusu tehditten kaç kullanıcının etkileneceğini ve hasar seviyesinin ne olacağını belirtmektedir. Dolayısıyla önceliğin belirlenmesinde bir tehdidin şiddeti ve etkisi önemsenmektedir.
- **İhtimal:** Söz konusu tehdidin gerçekleşme ihtimalini ifade etmektedir.
- **Farkındalık:** Kamuoyunun bir tehdit hakkındaki bilinç eksikliğini ifade etmektedir. Farkındalığın az olması bir tehdidin gerçekleşmeden önce tespit edilmesi ihtimalini azaltmaktadır.
- **Ar-Ge ihtiyacı:** Bir tehdidin azaltılması için ne tür yeni araştırmalara ihtiyaç olduğunu ifade etmektedir.

Bu faktörler dikkate alınarak yapılan önceliklendirmenin sonucuna göre en çok dikkat edilmesi gereken ilk beş tehdit (FORWARD, 2010):

- Çok çekirdekli işlemcilerle birlikte ardışık programlamanın yerini alan paralel programlama ile yeni açıklıkların ve tehditlerin ortaya çıkmasına yol açan **paralellik** kapsamındaki tehditler,
- Ağdaki cihazların çokluğu veya bir yazılım paketinin büyüklüğü ve karmaşıklığını ifade eden **ölçeğe** ilişkin tehditler,
- İnternetteki birçok saldırıyı destekleyen **yer altı ekonomisi destek yapılarına** ilişkin tehditler,
- Sayısı hızla artan mobil cihazları hedef alan **mobil kötücül yazılımlara** ilişkin tehditler ve
- Yüz milyonlarca kullanıcı tarafından kullanılan ve istismar edilebilen birçok kişisel bilginin paylaşıldığı **sosyal ağlarla** ilgili tehditler

şeklinde sıralanmaktadır (FORWARD, 2010).

Her bir siber tehdit yukarıda anlatılan dört faktöre göre değerlendirilerek düşük (D), orta (O) veya yüksek (Y) şeklinde sınıflandırılmaktadır. En sonunda ise her bir tehdit tüm faktörlere göre bütünsel olarak değerlendirilmekte ve son öncelik sınıfı belirlenmektedir (Tablo 1.2).

Tablo 1.2. Gelecekteki siber tehditlerin öncelik sınıfları

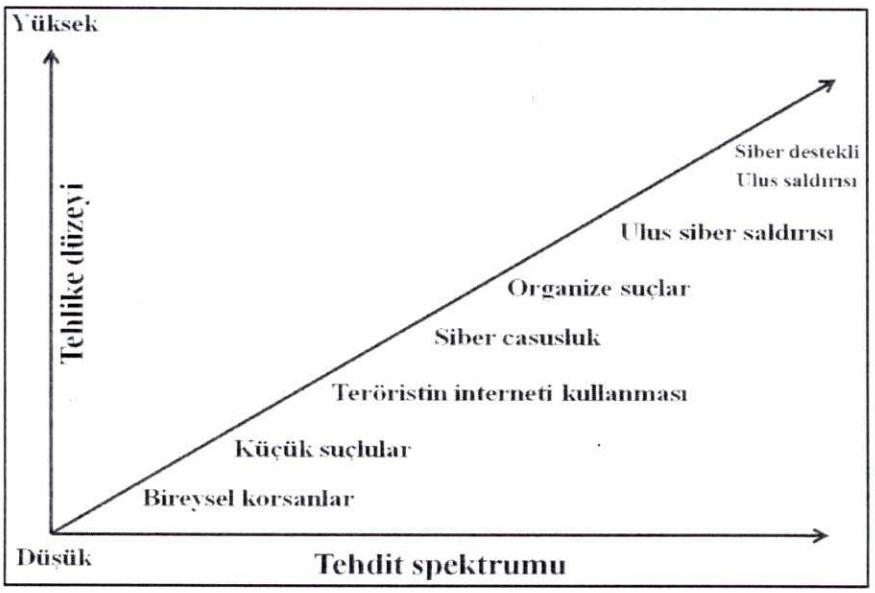
No	Siber tehdidin açıklaması	Etki	İhtimal	Farkındalık	Ar-Ge	Öncelik
1	Paralelliğe ilişkin tehditler (K)	O	O	Y	O	YÜKSEK ÖNCELİKLİ
2	Ölçeğe ilişkin tehditler (K)	Y	O	Y	O	
3	Yer altı ekonomisi destekleri (SA)	Y	Y	D	Y	
4	Mobil cihaz kötücül yazılımları (ZC)	Y	Y	O	Y	
5	Sosyal ağa ilişkin tehditler (VT)	Y	Y	O	Y	
6	Yönlendirme altyapıları	Y	Y	D	O	ORTA ÖNCELİKLİ
7	Hizmeti aksatma	Y	Y	D	O	
8	Kablosuz haberleşme	Y	Y	O	O	
9	Beklenmedik ard arda etkiler (K)	Y	O	Y	Y	
0	Yanlış sensör verileri	Y	O	Y	O	
1	Gizlilik ve yaygın sensörler	O	O	O	O	
2	Kullanıcı ara yüzü	O	Y	O	Y	
3	İçeriden gelen tehditler	Y	O	O	O	
4	Sistemin bakım kolaylığı ve doğrulanabilirliği (K)	O	Y	O	O	
5	Gizli işlevsellik (K)	O	O	Y	O	
6	Mağdurlara ulaşmak için yeni vektörler	O	Y	O	Y	
7	Sensörler ve RFID	O	Y	O	Y	
8	Gelişmiş kötücül yazılımlar	O	Y	O	O	
9	Sanallaştırma ve bulut bilişim	Y	O	Y	O	
0	Eski sistemlerin güvenliğinin güçlendirilmesi	O	O	O	D	
1	Yeni nesil ağlar	Y	Y	O	O	
22	IPv6 ve bilgisayarların doğrudan erişebilirliği	O	Y	O	O	DÜŞÜK ÖNCELİKLİ
23	Adlandırma ve kayıt kurumları (DNS)	D	Y	O	D	
24	Çevrim içi oyunlar	D	Y	O	D	

25	Emniyetin güvenlikten öncelikli olması	D	O	Y	O	
26	Hedefli saldırılar	O	Y	O	O	
27	Kötücül donanımlar	O	D	Y	O	
28	Ticari bileşenlerin kullanılması	O	Y	O	O	

Kaynak: (FORWARD, 2010)

Bir başka siber tehdit sınıflandırma çalışmasında kaynağına ve tehlike düzeyine göre bir sınıflandırma yapıldığı görülmektedir (Şekil 1.1).

Şekil 1.1. Siber tehdit kaynakları



Kaynak: (IBM, 2010)

Kaynağı ulus devlet olan siber destekli kinetik bir tehdidin en yüksek tehlike düzeyine sahip olduğu görülmektedir.

Kaynağına göre sınıflandırmanın dışında tehditlerin kullanılan teknik ve teknolojiye göre sınıflandırılması da mümkündür (Tablo 1.3).

Tablo 1.3. Kullanılan teknik ve teknolojiye göre tehdit sınıflandırması

Kategori	Açıklama	Örnekler
Bilgisayar korsanlığı	Çeşitli kontroller elde etmek amacıyla bir bilgisayara ya da ağa girme eylemi	• Yapısal sorgu dili (Structured Query Language - SQL) enjeksiyonu • Hizmeti aksatma • Varsayılan kimlik bilgileri üzerinden erişim
Kötücül yazılım	Sahibinin bilgisi veya onayı olmadan bir bilgisayar sistemine sızmak ya da zarar vermek için tasarlanmış yazılım.	• Klavye kaydetme ve casus yazılımları • Köle bilgisayar ağı • Solucan
Kötüye kullanma	Bilgi sistemlerinin istismar edilmesi.	• Sistem ayrıcalıklarının istismar edilmesi • Kendi çıkarı için kötüye kullanma
Aldatma ve sosyal ortam	Bir bilgisayara veya ağa yetkisiz erişim kazanmak için kullanıcının manipüle edilmesi eylemi.	• Yemleme • Yüz yüze • Telefon
Fiziksel	Bir bilgisayara veya ağ sistemine yetkisiz fiziksel erişim elde etmek veya tehdit etme eylemi.	• Telefonu dinleme • Omuzdan sörf • Saldırı veya zarar tehdidi

Kaynak: (IBM, 2010)

Bilgisayar korsanlığı örneklerinden olan SQL enjeksiyonu, hizmeti engelleme ve varsayılan kimlik bilgileri ile erişim tehditleri, çok çalışma gerektirmemesi, bu tehditleri saldırıya dönüştürecek araç ve gereçlere kolay ve ücretsiz ulaşılabilmesi dolayısıyla hemen her kullanıcı tarafından saldırıya dönüştürülmesi ihtimali yüksek olan tehditler arasında yer almaktadır.

Siber tehditlerin sınıflandırma çalışmalarından biri de kapsamlı, sistematik ve içerik tabanlı bir platform olan operasyonel olarak kritik tehdit, varlık ve açıklıkların değerlendirilmesi (Operationally Critical Threat, Asset, and Vulnerability Evaluation

- OCTAVE) platformudur. Carnegie Mellon Üniversitesinin bir hizmet markası olan OCTAVE, organizasyonların özellikle BİT altyapılarının gizlilik, bütünlük ve erişilebilirlik tehditlerinden korunmak için karar almalarına yardımcı olmaktadır (Alberts ve Dorofee, 2005).

OCTAVE'ye göre siber tehditler:

- Organizasyon için değer ifade eden bir **varlığı** hedef alması,
- Bir varlığın gizliliğini, bütünlüğünü ve erişilebilirliğini ihlal eden bir **aktörün** olması (içeriden veya dışarıdan olabilir),
- Aktörün bir kastının olup olmadığını ifade eden **niyeti**,
- Aktörün varlığa nasıl **erişim** sağlayacağı
- Varlığın güvenlik gereksinimleri ihlal etmenin ya da tehdidin gerçekleşmesinin **sonucu** (verileri ifşa etme, yok etme gibi)

gibi özelliklere sahiptir (Alberts ve Dorofee, 2005).

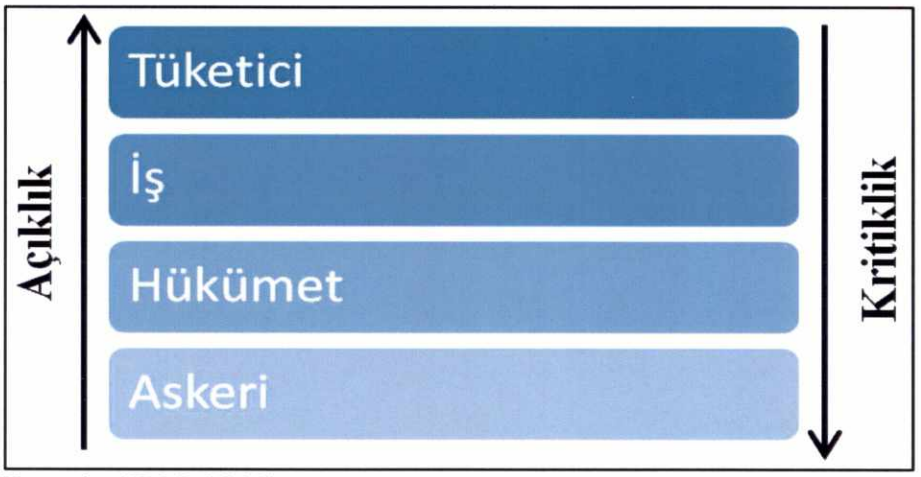
OCTAVE'nin sağladığı metot ile tehditlerin bilinen kaynaklarına ve sonuçlarına göre tehdit senaryoları üretilmekte ve teması ortak olan tehditler aynı grup altında gösterilmektedir. OCTAVE'ye göre dört standart tehdit kategorisi bulunmaktadır (Alberts ve Dorofee, 2005):

- **Ağ erişimi kullanan aktörler:** Bu kategoriye bir organizasyonun kritik varlıklarını hedef alan ağ tabanlı tehditler girmektedir. Bu tehditler ağa erişimi olan bir kullanıcının kasıtlı veya kazaen eyleme geçmesini gerektirmektedir.
- **Fiziksel erişimi kullanan aktörler:** Bir organizasyonun kritik varlıklarını hedef alan tehditler olarak tarif edilmektedir. Kişinin kasıtlı veya kazaen doğrudan müdahalesini gerektirmektedir.
- **Sistem sorunları:** Organizasyonun bilgi teknolojisi sistemlerindeki sorunlar bu kapsamda değerlendirilmektedir. Donanım arızaları, yazılım arızaları, ilgili kurumsal sistemlere erişilememesi, virüsler, kötücül kodlar ve diğer problemler bu kategoriye gösterilen örnekler arasında yer almaktadır.

- **Diğer problemler:** Organizasyonun kontrolü dışındaki tüm problem ve durumlar diğer problemler başlığı altında değerlendirilmektedir. Organizasyonun bilgi sistemlerini ve buna bağlı riskleri etkileyen sel ve deprem gibi doğal afetler örnek olarak verilmektedir.

Siber tehditlerin, hedef aldıkları kullanıcıları ve sistemleri seçerken nelere dikkat ettiklerinin, saldırı senaryosunun nasıl belirlendiğinin anlaşılmasının bir yönüyle BİT altyapılarının katmanlarına bağlı olduğu belirtilmektedir. BİT altyapılarının kritiklik düzeyinin artması ile sistemlerdeki güvenlik açıklıklarının azaldığı (Şekil 1.2), bu tür sistemleri hedef alan tehditlerin daha karmaşık ve daha organize olduğunu söylemek mümkündür. Bunun yanında çok sayıda güvenlik açıklığının bulunması ihtimali yüksek olan son kullanıcıya ait sistemleri hedef alan siber tehditlerin, bireysel korsanlar tarafından basit ve yaygın araçların kullanılması ile hayata geçirilmesi mümkün olabilmektedir (IBM, 2010).

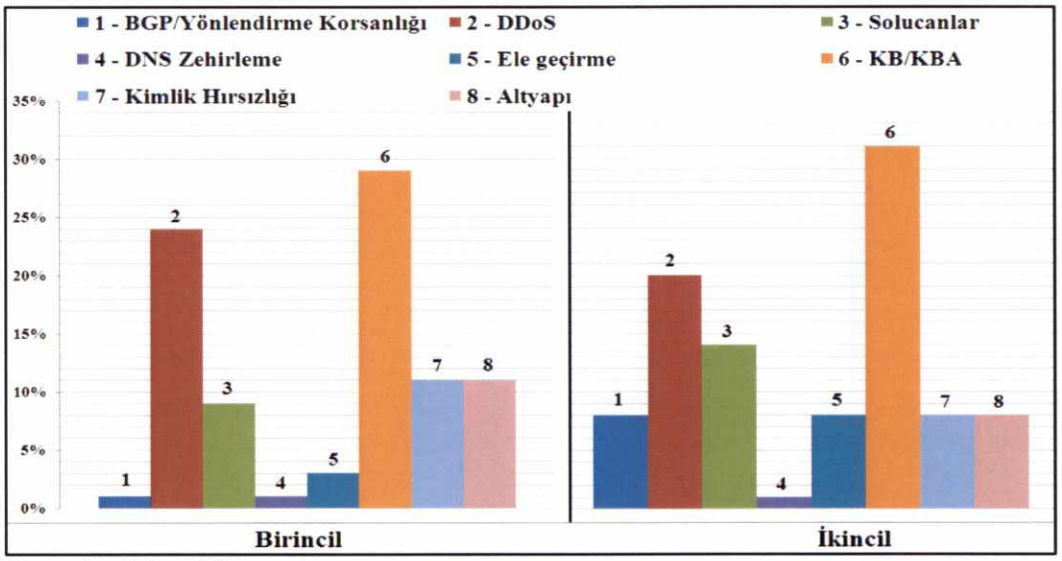
Şekil 1.2. BİT altyapı katmanları



Kaynak: (IBM, 2010)

Siber tehditlerin gerçekleşme oranları yapılan sıralama çalışmalarına bakıldığında, KBA'ların en çok endişe duyulan tehditler arasında ilk sırada, DDoS saldırılarının ise ikinci sırada yer aldığı görülmektedir (Şekil 1.3). KBA'ları DDoS tehdidi izlemektedir.

Şekil 1.3. En fazla endişe edilen tehditler

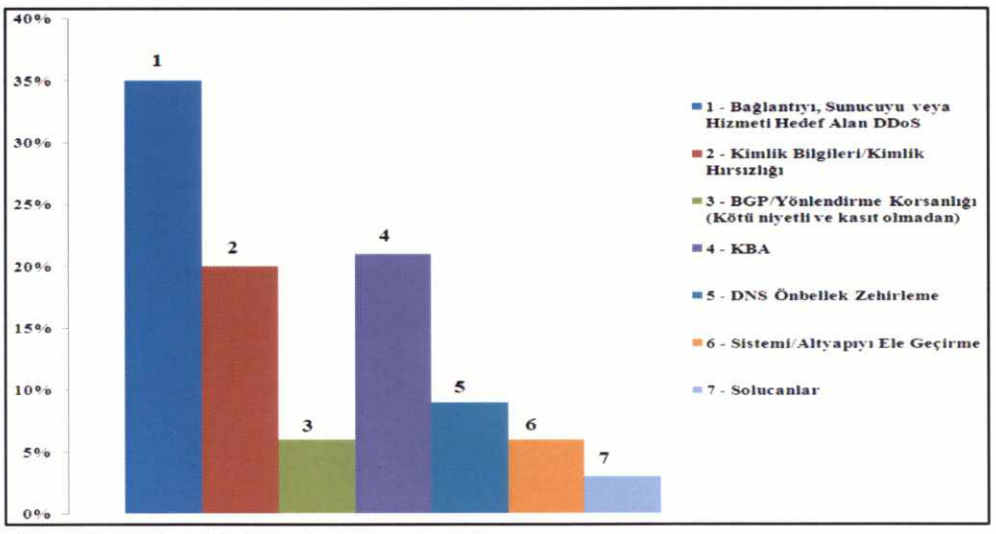


Kaynak: Arbor Networks

DDoS saldırılarının genellikle KBA'lardan kaynaklandığı düşünüldüğü için bu iki tehditten duyulan endişenin de paralel seviyelerde olduğu görülmektedir (Arbor Networks, 2007).

En büyük operasyonel sorunlara yol açmasından endişe duyulan tehditler incelemesinde ilk sırada bağlantıyı, sunucuları ve hizmetleri hedef alan DDoS saldırılarının (Arbor Networks, 2009) yer aldığı görülmektedir (Şekil 1.4).

Şekil 1.4. Beklenen en büyük tehditler



Kaynak: Arbor Networks

Yukarıdaki iki şekilde verilen bilgilerden, kullanıcıları özellikle de kuruluşları hedef alabilecek tehditlerin başında KBA'lar ve çoğunlukla KBA'ların kaynaklık ettiği DDoS saldırıları gelmektedir. Her iki tehdide yönelik önlemlerin alınmasının ve bu tehditlerin bertaraf edilmesinin kuruluşları önemli oranda rahatlatacağını söylemek mümkündür.

Özetlemek gerekirse, siber tehditlerin bazı çalışmalarda daha detaylı bazılarında ise daha genel başlıklar altında sınıflandırıldığı görülmektedir. Kurum ve kuruluşların genel güvenlik önlemleri almaları bağlamında detaya girmeyen kategorizasyonların hem maliyet açısından hem de personel yeterliliği açısından daha elverişli olabileceği değerlendirilmektedir. Bununla birlikte kurum ve kuruluşları yönlendirme ve koordine etme durumunda olan U-STİM'in tehditleri değerlendirirken detaya inmesinin etkin ve verimli çözüm önerilerinin geliştirilmesine katkı sağlayacağı düşünülmektedir.

Tehditleri detaylı bir şekilde sınıflandıran FORWARD çalışmasının sonuçlarına bakıldığında, yüksek öncelikli sınıfın ilk iki sırasında karmaşıklık kategorisinden ölçeğe ve paralelliğe ilişkin tehditler olmak üzere iki tehdidin bulunduğu görülmektedir. Karmaşıklık tehdit kategorisindeki diğer üç tehdit ise orta öncelikli sınıfa girmektedir. Dolayısıyla tehditlerin U-STİM penceresinden değerlendirilmesi durumunda, özellikle yüksek öncelikli sınıfa giren tehditlerle öncelikli olarak mücadele edilmesinin ve gerekli güvenlik önlemlerinin alınmasının etkin ve verimli bir yaklaşım olacağı değerlendirilmektedir. Özellikle hem yüksek öncelikli sınıfa hem de orta öncelikli sınıfa giren karmaşıklık kategorisindeki tüm tehditlerin dikkatle takip edilmesi ve konu ile ilgi gerekli çalışmaların yapılmasının da siber tehditlere müdahalede önemli bir aşama olduğu değerlendirilmektedir. Bunun yanı sıra U-STİM'in personeline eğitim ve kurs verilirken, güvenlik açıklıklarına ve siber tehditlere ilişkin bilgi toplama ve çözüm önerileri geliştirme çalışmaları sürdürülürken yüksek öncelikli sınıfa giren konulara ve karmaşıklık tehdit kategorisine öncelik ve önem verilmesinde yarar görülmektedir.

1.2. Siber Tehditlere Müdahale Merkezi

BİT'lerin toplum hayatını etkilemenin yanı sıra ülkelerin ekonomik ve sosyal hayatlarının önemli bir parçası haline gelmesi, bu sistemlerin bozulması veya imha edilmesi halinde toplumun hayati fonksiyonlarını olumsuz etkileyen kritik bilgi altyapısı olarak kabul edilmesine neden olmaktadır. BİT'lerin güvenliği ve erişilebilirliği kullanıcıları, kurum ve kuruluşları hatta devletleri giderek daha çok ilgilendirmektedir. Bu durumu siber tehditlerin ve olayların artışına, karmaşıklığına ve verdiği zararlara bağlamak mümkündür. Siber saldırılara ilişkin risklerin giderek büyümesi, bilinmeyen kaynaklardan gelen tehditlerin değişken bir yapıya bürünmesi ve sürekli gelişmesine paralel olarak, önemli siber olaylara medyada her zamankinden daha çok yer verilmesi dolayısıyla siber güvenlik konusunun daha etkin ve verimli bir şekilde ele alınması gerektiği sonucu çıkarılmaktadır (ENISA, 2010).

1988 yılında internet solucanının ortaya çıkmasından sonra Savunma İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency – DARPA) tarafından Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü'nde kurulan ve kurulduğu günden beri internet tabanlı olaylarla mücadele eden STİM/Koordinasyon Merkezini (CERT/Coordination Centre - CERT/CC) (Howard ve Longstaff, 1998) ilk siber olaylara müdahale merkezi olarak kabul etmek mümkündür.

Siber güvenlik olayları hakkında bilgi toplama ve bu olaylara karşı koymada koordinasyonu sağlama sorumluluğu olan STİM bu bağlamda önemli bir rol oynamaktadır. STİM'in amacı, herhangi bir siber tehdide veya siber olaya karşı, tehdidin hedef aldığı sistemleri korumak, saldırı durumunda olayı kontrol etmek ve oluşabilecek hasarları en aza indirmek, diğer ulusal ve uluslararası birim ve birliklerle olan koordinasyonu sağlamak, olaya ilişkin delilleri korumak, etkilenen sistemleri hızlı ve etkin bir şekilde yeniden çalışır duruma getirmek, sistemlerde tespit edilen açıklıkları gidererek benzeri olayların gelecekte tekrarlamasını önlemek ve organizasyonu hedef alan tehditlere ilişkin bilgiler elde etmektir.

STİM'ler başlangıçta özel sektörün bazı kesimlerine veya akademik çevredeki kullanıcılara güvenlik olaylarını yönetme hizmetleri vermek amacıyla kurulmuştur. Ancak zamanla olay yönetiminin ülke sınırları içinde yer alan geniş yelpazedeki sektörleri kapsayacak şekilde ulusal STİM'ler tarafından desteklenmesi ihtiyacı doğmuştur. STİM'ler siber güvenliğin sağlanmasında ve kritik altyapıların korunmasında ulusal seviyede ana merkez haline gelmektedir (ENISA, 2010).

STİM, siber güvenlik tehditleri ile mücadelede ve siber olaylara karşı koymada kullanıcılara karşı belirli bir sorumluluğu olan bir hizmet organizasyonu olarak tanımlanmaktadır. STİM'in siber güvenlik olaylarını ele almak için gerekli hizmetleri sunmak ve hizmet verdiği kullanıcılarına güvenlik ihlallerinden sonra geri kurtarma süreçlerinde destek vermek gibi görevleri bulunmaktadır. Riskleri azaltmak ve mücadele edilmesi gereken olay sayısını en aza indirmek için birçok STİM'in hizmet verdikleri kullanıcılarına önleyici ve eğitim hizmetleri de verdikleri görülmektedir (ENISA, 2010). Zira siber olaylar meydana gelmeden önce önleyici güvenlik önlemlerinin alınması, bilinen güvenlik açıklıklarının tespit edilerek giderilmesi ve güvenlik personeli başta olmak üzere tüm personele konu ile ilgili eğitim verilmesi ile esasında siber tehditlere müdahale edildiğini söylemek mümkündür (ENISA, 2010).

U-STİM'in görevleri arasında diğer ülkelerin STİM'leri ve uluslararası platformlar ile işbirliği kuran ve olay raporları ve açıklıklar hakkında bilgi paylaşımında bulunan ulusal temas noktası olarak hizmet vermek sayılmaktadır. Ülke içindeki koordinasyondan sorumlu tek temas noktası ve son çözüm makamı olarak da bilinmektedir. Bir ülkede U-STİM ile Kamu STİM'inden (Kamu-STİM) sadece birinin olması durumunda birçok örnekte birbirinin yerine görev yaptığı görülmektedir (ENISA, 2010).

Kamu-STİM'lerin genellikle hükümetin ve kamu kurumlarının bilgi ve iletişim ağlarının korunmasından sorumlu oldukları görülmektedir. Dolayısıyla bir Kamu-STİM'in hizmet verdiği kullanıcılar devlet ve diğer kamu kuruluşları olmaktadır. Askeri STİM'lerin kendilerine özgü yapıları gereği birçok durumda ayrı düşünülmektedir (ENISA, 2010).

Siber güvenlik perspektifinden bir U-STİM'in veya Kamu-STİM'in temel amacı, ulusal ve ekonomik güvenliği, devletin faaliyetlerinin ve kritik altyapıların devamını sağlamak olarak tarif edilmektedir. Bu nedenle bir U-STİM veya Kamu-STİM olayları genellikle ulusal düzeyde izlemekte, kritik altyapıları etkileyebilecek olayları tanımlamakta, kritik sistemlere sahip olan paydaşları siber tehditler hakkında uyarmakta, kamuda ve özel sektörde STİM'lerin kurulmasına destek vermektedir (ENISA, 2010).

STİM'lerin geleneksel internet ortamında kötücül faaliyetlere karşı mücadelede ve bilgi paylaşımında oldukça başarılı olduklarını söylemek mümkündür. Ancak yeni bir hizmet sunma modeli olarak ortaya çıkan bulut bilişimle birlikte, bulut hizmetinin sunulduğu platformların güvenliğinin sağlanması konusunda güvenlik uzmanlarının yeni bir takım zorluklarla karşı karşıya kalacağı düşünülmektedir. Hâlihazırda hizmet veren STİM'lerin, henüz yaygın bir kullanımı ve dolayısıyla siber saldırganlar için yeteri kadar cazibesi olmayan bulut bilişim hizmeti sağlayıcıları etkin şekilde destekleyip desteklemeyeceklerinin net olmadığı ifade edilmektedir. Bulut bilişimi hedef alan siber tehditlerin ve olayların sonuçlarının, siber saldırganların geleneksel modelde dağınık halde bulunan hedeflere toplu halde ulaşabilme fırsatı elde etmeleri sebebiyle geleneksel olaylardan çok daha ciddi sonuçlar doğurabileceği belirtilmektedir. Bu gerçekten hareketle Bulut Güvenlik Birliği (Cloud Security Alliance - CSA) tarafından BulutSTİM (CloudCERT) girişimi başlatılmıştır (CSA, 2011). İlerleyen yıllarda bulut bilişimin yaygınlaşması ile birlikte STİM çalışmalarının ve yapılanmalarının BulutSTİM benzeri yapılanmalar yönüne kayacağını söylemek mümkündür.

1.3. U-STİM Altyapısı

Siber saldırılara karşılık vermek için izleme ve uyarı sistemlerine ve siber olaylara karşı koyma yeteneğine ihtiyaç duyulmaktadır. Zira kuruluş içinde ve ulusal seviyede bilginin serbestçe paylaşılması, işbirliğinin ve koordinasyonun sağlanması söz konusu sistemlerin ve yeteneklerin olmasına bağlıdır. Ağları korumak ve siber tehditlerle başa çıkmak, koordinasyon içinde yürütülen ulusal faaliyetlerle mümkün olmaktadır. Muhtemel saldırılar ve alınması gerekli önlemler konusundaki farkındalığın arttırılması için devletin her kademesinin, özel sektörle, akademik dünyayla, bölgesel ve uluslararası organizasyonlarla işbirliği içinde olması önem arz etmektedir. Siber tehditlerle etkin bir şekilde mücadele edilirken, finansmanın, insan kaynağının, eğitimin, teknolojik yeteneğin, kamu-özel ilişkilerinin ve yasal gereksinimlerin de göz önünde bulundurulması gerekmektedir (ITU, 2007a).

Bir kuruluş siber saldırıya uğradığında veya kuruluşa bir sızma teşebbüsü olduğunda, meydana gelen olaya hızlı ve etkin bir karşılığın verilmesi, hem saldırının hedefi olan organizasyon için hem de söz konusu organizasyonun müşterileri için kritik bir öneme sahiptir. Saldırının fark edilmesi, analiz edilmesi ve olaya karşılık verilmesi ne kadar hızlı ve dikkatli yapılırsa, oluşabilecek hasarları ve kurtarma maliyetleri, benzer olayların gelecekte tekrar yaşanması ihtimali o ölçüde azaltılmış olmaktadır. Dolayısıyla kullanıcılara güvenli bir siber ortam sunmada, oluşabilecek siber olaylara hızlı ve etkin bir şekilde müdahale edebilme yeteneğine sahip olmak çok önemli bir gereksinimdir. Bu gereksinimi karşılayabilecek çözümlerden biri resmi bir olaylara müdahale yeteneğinin veya ekibinin oluşturulmasıdır.

Bölgesel birçok girişimin, Uluslararası Telekomünikasyon Birliği'ne (International Telecommunication Union - ITU) üye devletlerin U-STİM gibi ulusal siber güvenlik olaylarına karşı koyma merkezi kurmalarını önerdiği ifade edilmektedir. Birçok ülkenin özellikle de gelişmekte olan ülkenin bu konuda yeterince hazırlıklı olmadığı tespitine yer verilmektedir. Dolayısıyla bu ülkelerin BİT'lerinden kaynaklanabilecek bir saldırının diğer birçok ülkenin sistemlerini de etkileyebileceğinden endişe edilmektedir. Bu noktadan hareketle ITU'nun ITU WTSA-08 586 numaralı kararı ile konuya vurgu yapılmakta, ITU üyesi devletler ulusal U-STİM'lerini kurmaları

hususunda teşvik edilmektedir. Siber tehditlerle mücadelede her ülkede bir seviyenin yakalanmasının ve hazırlıklı olunmasının, U-STİM kurulması ihtiyacının ve bölgeler arasındaki koordinasyonun sağlanmasının önemi dolayısıyla bu alanda yardıma ihtiyaç duyan devletlerin ITU'ya başvurmaları istenmektedir (ITU, 2007a).

Olaylara müdahale ekibinin görevleri arasında, bir siber olay meydana geldiğinde organizasyonda oluşabilecek hasarları en aza indirmek, olay gerçekleşirken oluşan delilleri korumak, sistemleri hızlı ve etkili bir şekilde yeniden çalışır duruma getirmek, gelecekte benzer olayların meydana gelmesini önlemek ve organizasyonu hedef olan tehditlerin detaylarını araştırmak sayılmaktadır (Cisco, 2010).

1.3.1. STİM yapısı

STİM'lerin varlığı yaklaşık 20 yılı bulmasına rağmen, bir yapının STİM olup olmadığına karar vermek için henüz yaygın kabul görmüş bir tanım bulunmamaktadır. Ancak CERT/CC'nin yayımlamış olduğu STİM el kitabında (CSIRT Handbook), "Bir takımın STİM olarak kabul edilebilmesi için, bu takımın siber olayların ele alınmasına ilişkin olay analizi, olaya yerinde müdahale, olaya müdahale desteği veya olaya müdahale koordinasyonu hizmetlerinden en az birini sunuyor olması gerekmektedir.". Bu tanım dikkate alındığında bu hizmetlerden birini sunan bir STİM reaktif kabul edilmektedir (Wiik ve Kossakowski).

Siber tehditlere müdahale yapıları, "güvenlik ekipleri", dâhili STİM'ler ve koordine STİM'ler şeklinde sınıflandırılmaktadır. Güvenlik ekiplerinde, olaylara müdahale için organizasyondaki herhangi bir grup görevlendirilmemekte ve kurulu bir STİM bulunmamaktadır. Bunun yerine, o birimde çalışan ve genellikle sistem, ağ ve güvenlik yöneticilerinden oluşan mevcut personelin, rutin işlerinin bir parçası olarak güvenlik olaylarına geçici bir şekilde müdahale etmeleri söz konusu olmaktadır. Dâhili bir STİM'de, güvenlik olayları belirli kişilerden oluşturulmuş bir grup tarafından ele alınmaktadır. Söz konusu STİM, hizmet verdiği organizasyonun içinde yer almaktadır. Bu modelde her kurumun veya kuruluşun kendi bünyesinde ve

sadece kendi organizasyonuna hizmet verecek bir STİM'in varlığı söz konusudur (Alberts vd. , 2004).

Koordine STİM (K-STİM) modelinde ise STİM, güvenlik olaylarının, güvenlik açıklarının ele alınmasında ve dâhili ve harici çeşitli organizasyonlar arasındaki bilgi paylaşımında koordinasyonu sağlamaktadır. Amerika Birleşik Devletleri'nde (ABD) bulunan CERT/CC ve Avustralya'daki AusCERT K-STİM'e gösterilebilecek örnekler arasında yer almaktadır (Alberts vd., 2004).

Güvenlik konularının yönetilmesi için STİM gibi özel bir ekibin olması bir organizasyona değerli varlıklarını korumada, özellikle büyük ölçekli siber tehditleri önlemede ve bunlarla mücadele etmede yardımcı olmaktadır. Bu tür bir ekibin olması:

- Organizasyon bünyesinde güvenlik sorunları ile ilgilenmek için merkezi bir irtibat noktasının olması,
- Güvenlik olaylarının merkezi ve uzman bir birim tarafından ele alınması ve bu olaylara karşı koyulması,
- Güvenlik olaylarını hızlı bir şekilde bertaraf etmeleri konusunda kullanıcılara destek verebilecek uzmanlık düzeyine sahip olunması,
- Hukuki konular ile ilgilenilmesi ve bir dava durumunda delillerin muhafaza edilmesi,
- Siber güvenlik alanındaki gelişmelerin takip edilmesi,
- Bilgi teknolojilerinin güvenliği konusunda müşteri kurum ve kuruluşlar arasında işbirliğinin teşvik edilmesi

gibi yararlar sağlamaktadır (ENISA, 2006a).

Sonuç olarak siber tehditlere müdahalede hem organizasyonlara hem de kullanıcılara teknik ve hukuki yararlar sağlayan, tek bir koordinasyon merkezi olması dolayısıyla etkin ve verimli bir müdahale fırsatı sunan STİM gibi özel bir güvenlik ekibinin olmasının gerektiği düşünülmektedir.

STİM yapısının oluşturulması çalışmalarında dikkate alınması gereken bazı hususlar bulunmaktadır:

- Düzenleme kapsamları telekomünikasyondan BİT'lere doğru genişleyen düzenleyici kurumlar STİM konusunda da çalışmalar yürütmektedirler.
- Doğası gereği siber tehditlerin birçok tarafı ilgilendirmesinden dolayı konu ile ilgili farklı paydaşların yürüttükleri farklı görevler olabilmektedir. STİM çalışmalarına devletin öncülük etmesi, olabildiğince çok paydaşın katılımının sağlanması, söz konusu paydaşların görev ve sorumluluklarının hukuki düzenlemelerle belirlenmesi önem arz etmektedir.
- Bununla birlikte yürütülecek çalışmaların kapsamının belirlenmesi açısından, STİM'in siber tehditlerden korunma konusunda müşteri kurum veya kuruluşlara hangi misyonla hizmet sunacağının belirlenmesi de gerekmektedir.
- STİM'in hangi organizasyon yapısı ile yapılandırılacağı, büyüklüğünün ve personel sayısının ne olması gerektiği, sunulacak hizmetler ve hizmet sunulacak müşteriler açısından önem arz etmektedir.
- STİM müşterilerinin ve sunulabilecek hizmetlerin belirlenmesinden sonra faaliyetlerin sürdürülebilirliği için STİM'in finansal yapısının tasarlanması gerekmektedir.

Bu bölümde yukarıda bahsedilen hususlar incelenmektedir.

1.3.1.1. STİM ve düzenleyici kurumlar

Bilgi ve ağ güvenliği alanındaki artan rolleri ile düzenleyici kurumlar:

- Yetki çerçevesinin uygulanması,
- Rekabetin sağlanması,
- Şebekelerin ve tesislerin birbirine bağlanması,
- Evrensel hizmet ve erişim mekanizmalarının uygulanması,
- Radyo spektrumunun yönetilmesi

gibi görevleri ile elektronik haberleşme sektörünü rekabete açmayı hedeflemişlerdir. Bununla birlikte teknolojinin gelişmesine paralel olarak hem düzenleyici kurumların

rolü gelişmiş hem de BİT'lerin kullanımı önemli oranda artmıştır. Bu artış düzenleyici kurumların daha fazla ön planda yer almasına yol açmıştır. Birçok ülkede düzenleyici kurumlar BİT politikalarının şekillenmesinde önemli rol oynamaktadır. Bazı ülkelerde bu kurumların BİT sektörünü yönettikleri ve bu sektörün gelişmesini teşvik ettikleri de bilinmektedir. Dolayısıyla düzenleyici kurumların düzenleme kapsamlarının telekomünikasyondan BİT'lere doğru genişlediğini söylemek mümkündür (ITU, 2009).

BİT'lerin daha çok erişilebilir olmaya başlaması ile birlikte birçok düzenleyici kurumun kapasitenin arttırılması, tüketicinin korunması ve farkındalığın arttırılması konularında da rol aldıkları gözlemlenmektedir. Bu durum düzenleyici kurumların, artan siber güvenlik problemleri ile mücadele etmek için görev, kaynak ve deneyim bakımından daha iyi bir duruma gelmelerine yol açmıştır (ITU, 2009).

Siber güvenlik ihtiyacının ortaya çıkması ile birlikte düzenleyici kurumlar siber güvenlik konularında da rol almaya başlamışlardır. Bu alanda düzenleyici kurumlar tarafından yürütülen çalışmalar arasında, siber olayların yönetilmesi ve siber güvenlik hazırlık değerlendirmesi çalışmaları yer almaktadır. Siber olayların yönetimi konusunda bazı düzenleyici kurumlar aşağıda yer alan rolleri üstlenmişlerdir (ITU, 2009):

- Bazı düzenleyici kurumlar ulusal siber olayların izlenmesi için gerekli altyapıları kurmuşlardır. Örneğin İsveç düzenleyici kurumu 2002 yılında bilgi teknolojisi olayları merkezi adıyla STİM işlevi gören bir yapı kurmuştur.
- Yine çeşitli düzenleyici kurumlar, APCERT gibi bölgesel veya FIRST gibi uluslararası siber olay izleme girişimlerine katılım sağlamışlardır.

1.3.1.2. Yasal dayanak

Hukuki düzenleme çalışmalarında devlet düzenlemesi, öz düzenleme ve ortak düzenleme olmak üzere üç farklı düzenleme modelinden bahsetmek mümkündür. Siber tehditler ve siber olaylar doğası gereği birçok tarafı ilgilendirdiği için konu ile ilgili farklı paydaşların yürüttükleri farklı görevler olabilmekte ve bu alanda yapılan

hukuki düzenlemelerde benimsenen düzenleme modeli, tarafların konu ile ilgisini belirlemede önemli bir yapıtaşı olarak görülmektedir. Bu noktadan hareketle düzenleme modellerinden ortak düzenleme ve öz düzenleme modelleri ile daha fazla paydaşın siber âleme ilişkin düzenleme süreçlerinde yer almaya başladığı gözlemlenmektedir (ITU, 2010).

Siber tehditlerin etkilediği farklı alanların ve hizmetlerin düzenlenmesi, düzenleme alanlarının çakışmasına yol açabilmektedir. Bu durumda sadece ulusal seviyedeki farklı düzenleyici kuruluşlar arasında değil aynı zamanda uluslararası düzeyde de işbirliğine gereksinim duyulmaktadır. Dolayısıyla operasyonel anlamda kurulmasında yarar görülen ve teşvik edilen kamu-özel sektör işbirliği yaklaşımının düzenleme modeli seçiminde de dikkate alınması gerektiği değerlendirilmektedir (ITU, 2010).

Demokratik meşruiyet ve doğrudan uygulanabilirlik bağlamında devletin siber âleme ilişkin düzenlemelerin dışında tutulamayacağı, bununla birlikte teknik ve operasyonel problemlerin olduğu dikkate alındığında devlet düzenlemesinin öz düzenleme veya ortak düzenleme gibi farklı bir modelle desteklenmesi ihtiyacı duyulmaktadır (Bakırcı, 2010).

Diğer taraftan devlet düzenlemesinde ortaya çıkan problemlerin giderilmesi amacıyla ortaya çıkan öz düzenleme, esnek ve maliyet etkin bir yapıya sahip olmasına karşın, yaşanan ihlallere yeterli yaptırımların uygulanamaması başta olmak üzere çeşitli zayıflıkları bünyesinde barındırmaktadır. Dolayısıyla öz düzenlemenin devlet düzenlemesi ile desteklenmesi gerektiği değerlendirilmektedir (Bakırcı, 2010).

Siber âlemde paydaşlar arasındaki işbirliğinin öneminden hareketle çok paydaşlı ortaklık fikrinin, öz düzenleme ve devlet düzenlemesinin olumlu taraflarını içeren olumsuz yanlarını ise kontrol eden ortak düzenleme modeli ile sağlanmış olacağı düşünülmektedir (Bakırcı, 2010).

Sonuç olarak, siber tehditlerle etkin ve verimli bir mücadele için STİM yapısına ilişkin düzenleme yapılırken konu ile ilgili tüm paydaşların yürütülecek çalışmalarda yer almasını sağlamak üzere ortak düzenleme modelinin benimsenmesinin yararlı olacağı değerlendirilmektedir.

1.3.1.3. Misyon ve müşteri

STİM'in sunduğu hizmetlerden yararlanan bireysel veya kurumsal taraflar müşteri olarak adlandırılmaktadır. Müşteri, farklı sayıdaki birimlerden oluşabileceği gibi tek bir merkezden de oluşabilmektedir. Doğru kişilere hizmet sunulabilmesi için müşterilerin iyi bir analiz çalışması ile belirlenmesinde yarar görülmektedir (Killcrece vd., 2003b).

Müşteri analizi, hizmet sunulacak kuruluşların yapısı, fiziksel veya coğrafi konumu ve sektörü göz önünde bulundurularak STİM'in organizasyonel modelinin belirlenmesine katkı sağlayan bir süreçtir. Organizasyon yapısı sadece bir birimden oluşan müşteri ile bir ağ üzerinden haberleşen ve birden fazla lokasyonu olan müşterinin STİM'e duyacağı ihtiyaç farklılık arz etmekte, dolayısıyla STİM'in organizasyonel yapısı da buna göre şekillenebilmektedir (Killcrece vd., 2003a).

Müşteri tanımının yapılmasında dahili veya harici, merkezi ya da dağıtık gibi ayırt edici bazı organizasyonel faktörlerden bahsetmek mümkündür. Dâhili organizasyon yapısında STİM, müşteri ile aynı yapı içerisinde yer alırken harici yapıda müşteri ile farklı organizasyonel yapıların altında yer almaktadır. STİM ve müşterinin aynı binada yer alması gibi fiziksel veya coğrafi olarak birbirine yakın olması merkezi yapıyı, birbirine uzak ayrı binalarda, şehirlerde, ülkelerde veya farklı zaman dilimlerinde yer alması ise dağıtık yapıyı ifade etmektedir (Killcrece vd., 2003a).

STİM'in hizmet vereceği kurumların veya kuruluşların belirlenmesinde sektörel temelli bir sınıflandırma da yapılabilmektedir. Sektörel temelde; akademik birimlere, ticari kuruluşlara, kritik altyapılara, devlet birimlerine, dâhili birimlere, askeri birimlere, ulusal kurumlara/kuruluşlara, küçük ve orta ölçekli işletmelere, bayi veya

satıcılara şeklinde bir sınıflandırmaya tabi tutulan sektörlere hizmet veren STİM'ler şeklinde bir sınıflandırma yapılmaktadır (ENISA, 2006a,).

U-STİM'in genelde doğrudan hizmet verdiği müşterileri bulunmamakta, daha çok ülke genelinde aracı bir nokta veya koordinasyon merkezi olarak hizmet vermektedir. Bazı ülkelerde bir STİM'in hem Kamu-STİM hem de U-STİM rolü ile hizmet vermesi söz konusu olabilmektedir.

STİM'in misyonunun, temel amacının ve işlevinin kısa ve açık bir şekilde ortaya koyulması gerekmektedir. Misyon ile güvenlik ekibinin sistemlerin geri kurtarılması, saldırıların ve sızmaların analizi, karşı koyma faaliyetlerinin koordine edilmesi ve kolaylaştırılması, siber suçların soruşturulması, saldırı tespit sistemlerinin izlenmesi gibi temel çalışma alanları belirlenmiş olmaktadır (Killcrece vd., 2003a).

Misyon ve verilecek hizmetler, STİM'in organizasyonel modelini de etkilemektedir. Zira bir güvenlik ekibin geri kurtarma faaliyetlerini bizzat gerçekleştirmesi söz konusu ise, ekibin kurtarılacak sistemlerin bulunduğu bölgeye erişmesi gerekmektedir (Killcrece vd., 2003a).

STİM'in yapısının belirlenmesinde etkili olan müşteri kurum ve kuruluşların belirlenmesini ve analiz edilmesini, STİM çalışmalarının başarılı olmasının ilk adımları olarak değerlendirmek mümkündür. Dolayısıyla hizmet verilecek müşterilerin belirlenmesi ve kaliteli hizmetlerin sunulması için müşteri ihtiyaçlarının belirlenmesi önem arz etmektedir. STİM'in misyonunun da bu ihtiyaçlar doğrultusunda olması gerekmektedir.

1.3.1.4. Organizasyon yapısı

Daha önce de bahsedildiği üzere STİM'in yapısı, bünyesinde yer aldığı organizasyonun ve hizmet vereceği müşterilerin mevcut yapılarına bağlıdır. Bunun yanı sıra yapı, kalıcı veya geçici olarak çalıştırılabilecek yetenekli uzmanlara sahip olup olmamaya bağlı olarak da değişebilmektedir (ENISA, 2006a).

STİM ekibinde özellikle başlangıç aşamasında, uzman bir hukukçunun yer almasının oldukça yararlı olduğuna vurgu yapılmaktadır. Bunun maliyetleri arttıracağı düşünülse de zamanın verimli kullanılması ve muhtemel yasal sorunların en aza indirilmesi söz konusu olmaktadır (ENISA, 2006a).

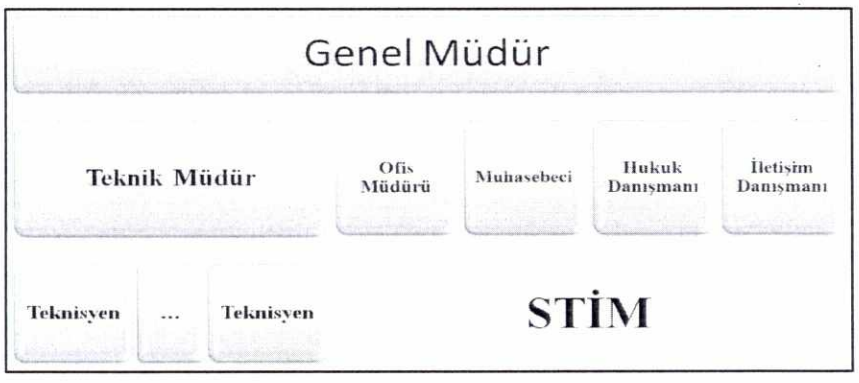
Müşterilerin farklı uzmanlık alanlarının olması ve verilen hizmetlerin kritik olmasından dolayı STİM'in medyada yer alabileceği düşünülerek ekip içerisinde bir iletişim uzmanına yer verilmesinin yararlı olacağı değerlendirilmektedir. İletişim uzmanlarından, anlaşılması zor teknik konuları müşterilerin veya medya mensuplarının kolaylıkla anlayabilecekleri mesajlara dönüştürmeleri, bunun yanı sıra müşterilerden alınan geri bildirimleri STİM'in teknik uzmanlarına sunmaları beklenmektedir. Dolayısıyla iletişim uzmanı STİM personeli ile müşteriler ve medya arasındaki haberleşme köprüsü olacaktır (ENISA, 2006).

STİM'in organizasyon yapısı, kullanılacak olan iş modelini de etkilemektedir. Hali hazırda STİM'ler tarafından kullanılan çeşitli organizasyonel iş modelleri bulunmaktadır.

a. Bağımsız iş modeli

Bağımsız iş modelinde STİM kendi yönetimi ve çalışanları olan ayrı bir organizasyon olarak faaliyet göstermektedir (Şekil 1.5).

Şekil 1.5. STİM - bağımsız iş modeli

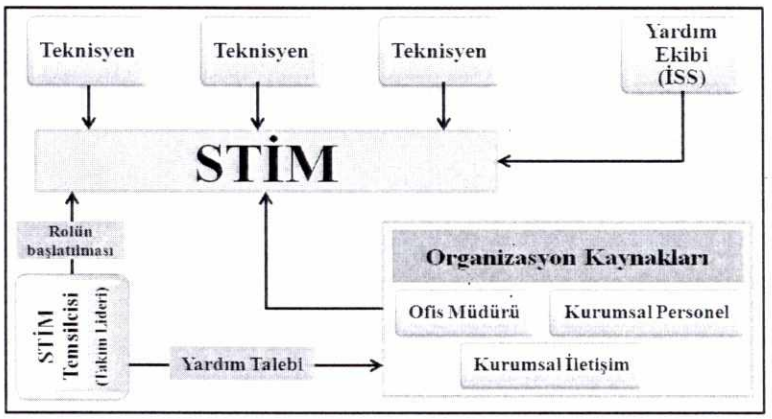


Kaynak: (ENISA, 2007)

b. Gömülü iş modeli

Bir STİM'in mevcut bir organizasyonun bünyesinde kurulması ve var olan bilgi teknolojileri biriminin kullanılmak istenmesi durumunda gömülü STİM modelinin kullanılması önerilmektedir. Bu modelde STİM ekibi bir takım lideri tarafından yönetilmekte (Şekil 1.6) ve STİM'in faaliyetlerinden takım lideri sorumlu tutulmaktadır (ENISA, 2006a).

Şekil 1.6. STİM - gömülü iş modeli

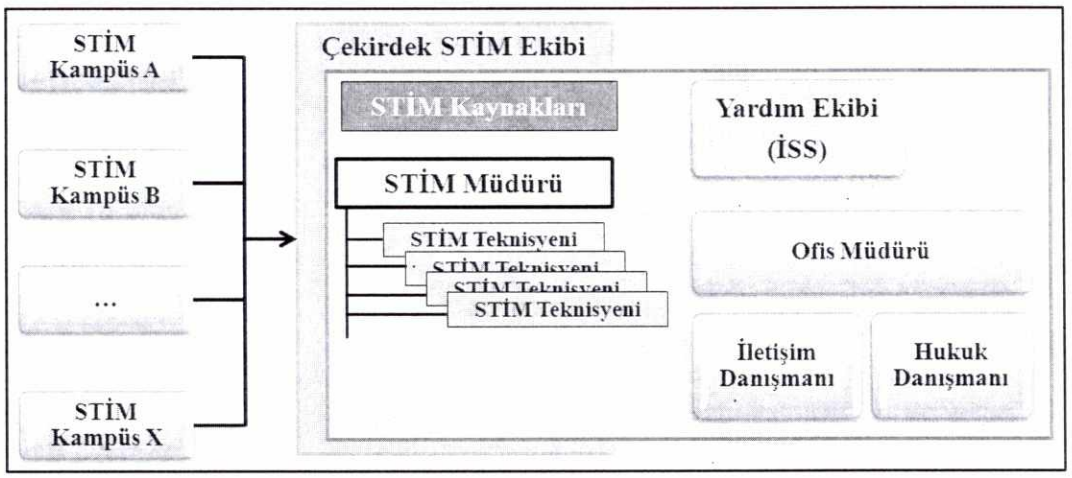


Kaynak: (ENISA, 2006a)

c. Kampüs iş modeli

Akademik ve araştırma organizasyonları birçok farklı bölgede yer alan üniversitelerden ve kampüslerden oluşmaktadır. Kampus modeli de çoğunlukla akademik ve araştırma alanlarında hizmet veren STİM'ler tarafından kullanılan bir iş modelidir. Genellikle bu organizasyonlar birbirinden bağımsız olarak faaliyet göstermekte ve kendi STİM'lerini kurmaktadırlar. Her organizasyonun kurduğu bu bağımsız STİM'ler çekirdek bir STİM'in şemsiyesi altında toplanmaktadır. Çekirdek STİM koordinasyon ve dış dünya için yegâne temas noktası olarak hizmet vermektedir (Şekil 1.7).

Şekil 1.7. STİM - kampüs iş modeli



Kaynak: (ENISA, 2007)

Çekirdek STİM'ler iş yüklerini ve maliyetlerini azaltmak amacıyla bazen verdiği hizmetleri kampüs STİM'lere devredebilmektedir (ENISA, 2006a).

d. Gönüllülük esasına dayalı iş modeli

Gönüllük esasına dayalı iş modelinde bir grup uzman bir araya gelerek birbirlerine ve diğer insanlara gönüllü olarak tavsiye ve destek sağlamaktadır. Bu modelde katılımcıların motivasyonlarına bağımlılık söz konusudur (ENISA, 2006a).

1.3.1.5. Personel yapısı

STİM ekibinin büyüklüğünün ne olması gerektiği konusunda net bir görüş olmamakla birlikte personel sayısı, personelin uzmanlık düzeyine, meydana gelen siber olay sayısına ve sunulan hizmet türlerine göre değişiklik gösterebilmektedir (Killcrece vd., 2003b).

Verilecek hizmetlerin ve sağlanacak desteğin seviyesinin belirlenmesi ve uygun organizasyonel modelin seçilmesi istihdam edilecek personel konusunda bir fikir vermektedir. Söz konusu hizmetler ve destek ancak yeterli sayıdaki ve uzmanlıktaki personel ile verilebilecektir (ENISA, 2006a).

İhtiyaç duyulan personelin sağlanması her zaman mümkün olamamakla birlikte etkin bir takım oluşturabilmek için dikkat edilmesinde yarar görülen bazı noktalar bulunmaktadır:

- Temel STİM hizmetlerinden tavsiye bültenlerinin yayınlanması ve güvenlik olaylarının ele alınması hizmetlerini sunabilmek için en az 4 adet 7/24 çalışana,
- Çalışma saatleri içerisinde STİM hizmeti verebilmek ve sistemlerin bakımını yapabilmek için en az 6–8 adet 7/24 zamanlı çalışana,
- Çalışma saatleri dışında 7x24 iki tam vardiya ile hizmet verebilmek için en az 12 7/24 çalışana

ihtiyaç duyulmaktadır. Rakamlar hastalık ve tatil gibi durumlar düşünülerek yedekli olarak verilmektedir (ENISA, 2006a).

Personel sayısının meydana gelen siber olayların sayısına, personelin deneyimine bağlı olduğu ve siber olayların sayısının tahmin edilmesinin zorluğu dikkate alındığında, bu zorlukların ancak STİM'in dinamik bir personel rejimine sahip olması ile aşılabileceği değerlendirilmektedir.

1.3.1.6. Ekipmanlar ve araçlar

STİM'lerin ofis ve ekipman ihtiyaçları farklılık göstermekle birlikte her STİM'de olmasında yarar görülen temel bazı noktaların olduğunu söylemek mümkündür. Ofis binasının, STİM faaliyetleri yürütülürken kullanılan bilgi teknolojileri araçlarının ve kullanılan iletişim kanallarının sahip olması gereken çeşitli kriterler bulunmaktadır (ENISA, 2006a).

a. Binanın güçlendirilmesi

STİM'lerin çok hassas bilgileri işlediklerinden dolayı bu bilgilerin fiziksel güvenliğinin sağlanması büyük önem arz etmektedir. Ancak bu durum organizasyonun mevcut tesislerine, altyapısına ve bilgi güvenliği politikasına bağlıdır.

STİM binasının;

- Binaya girişlerin kontrollü bir şekilde yapılabilmesi,
- Sadece STİM personelinin girebilmesi,
- Ofislerin ve girişlerin kamera ile görüntülenebilmesi,
- Gizlilik arz eden bilgilerin kilitli dolaplarda veya güvenliğinin bir şekilde sağlanarak saklanabilmesi,
- Güvenli bilgi teknolojileri sistemleri kullanılması

özelliklerine sahip olması önerilmektedir (ENISA, 2006a).

b. Kullanılan bilgi teknolojisi araçları

STİM bünyesinde;

- Çalışan personelin teknik desteğini verebileceği araçların kullanılmasına,
- İnternete bağlamadan önce tüm sistemlerin yamalarının ve güncellemelerinin yapılmasına,
- Güvenlik duvarı, birden fazla antivirüs programı gibi güvenlik yazılımlarının kullanılmasına

özen gösterilmesi gerekmektedir (ENISA, 2006a).

c. İletişim kanalları

İletişim kanalları oluşturulurken;

- Umumi bir internet sayfasının olmasının,
- İnternet sayfasında üyelere özel alanların olmasının,
- Güvenlik olaylarının rapor edilebilmesi için internet sayfasında formların yer almasının,
- Çok iyi gizlilik (Pretty Good Privacy - PGP) veya Güvenli / Çok Amaçlı Elektronik Posta Uzantıları (Secure/Multipurpose Internet Mail Extensions - S/MIME) destekli elektronik postanın kullanılmasının,

- Elektronik posta listesi yazılımı kullanılmasının,
- Müşterilerin erişebilmeleri için hazır tutulan bir, telefon, faks ve kısa mesaj servisi (KMS) numarasının olmasının

yararlı olacağı değerlendirilmektedir (ENISA, 2006a).

d. Kayıt tutma sistemleri

STİM faaliyetlerinin yürütülmesinde;

- STİM ekip çalışanlarının ve diğer STİM'lerin iletişim bilgilerinin yer aldığı iletişim veritabanının,
- Müşteri ilişkileri yönetim araçlarının,
- Güvenlik olaylarının ele alınması işlemlerinde biletleme veya etiketleme sistemlerinin

kullanılması katkı sağlamaktadır (ENISA, 2006a).

e. Kurumsal tarzın benimsenmesi

STİM'in kurulmasından itibaren kurumsal tarzın benimsenmesinin önemli olduğu belirtilmektedir. Kurumsal bir tarz ile hizmet sunmak, müşterilerde STİM'e karşı bir güvenin oluşmasına ve bu güvenin sürmesine katkı sağlayacaktır (ENISA, 2006a).

1.3.1.7. Finansal yapı

STİM tarafından sunulabilecek hizmetlerin ve bu hizmetlerden yararlanacak müşterilerin belirlenmesinin ardından, hizmeti uygun ve karlı bir şekilde sunabilmek için STİM'in finansal yapısının çok iyi tasarlanması gerekmektedir.

Bir STİM'in kurulması ve işletilmesi için ihtiyaç duyulacak bütçenin büyüklüğünün belirlenmesi, o anki piyasa koşullarına ve takımın kuruluş yapısına bağlıdır. Örneğin kuruluş içerisinde yer alan dağıtık bir ekip için ilave maaş ödenmesine veya ekipman satın alınmasına gerek olmayabilmektedir. Oysa tesisleri ayrı olan yeni bir ekibin kurulması durumunda daha çok bütçeye ihtiyaç duyulacaktır. STİM'in kuruluş

giderleri dışında personel giderleri de bulunmaktadır. STİM çalışmaya başladığı andan itibaren işletim giderleri ve personel maliyetlerini karşılayabilmek için sürdürülebilir bir bütçeye ihtiyaç duyacaktır (Killcrece vd., 2003b).

STİM'lerin çoğunlukla bir üniversite, ticari kuruluş, askeri kuruluş veya devlet kurumu tarafından finanse edildikleri gözlemlenmektedir. Ancak AusCERT gibi hizmet sunduğu müşterilerinden üyelik aidatı alarak, Kanada STİM'i olan CanCERT gibi sunduğu hizmet başına ücret alarak gelir sağlayan STİM'ler de bulunmaktadır (Killcrece vd., 2003b).

Normal şartlarda finansmanın müşteri ihtiyaçlarına göre belirlenmesi beklenmektedir. Ancak gerçekte verilen hizmetlerin mevcut bütçeye göre ayarlanması söz konusu olmaktadır. Dolayısıyla STİM'in yapısının tasarlanmasına parasal konulardan başlamanın daha gerçekçi ve etkili olacağı sonucuna varmak mümkündür (ENISA, 2006a). Bu amaçla maliyet ve gelir modelinin iyi tasarlanması gerekmektedir.

a. Maliyet modeli

Maliyetleri arttıran faktörlerin en önemlileri arasında verilecek hizmetin saatleri ve istihdam edilecek personel sayısı sayılmaktadır. Güvenlik olaylarına müdahale ve teknik destek sağlamak için 7x24 hizmet vermenin gerekliliğinin iyi analiz edilerek hizmet sunulacak saatlerin belirlenmesi maliyetler açısından önem arz etmektedir. Bazı hizmetlerin çalışma saatleri içerisinde sunulmasının yeterli olup olmayacağını incelemek gerekmektedir. İstenilen erişilebilirlik ihtiyacına ve ofis araçlarına bağlı olarak çağrı üzerine veya planlı bir programa bağlı bir şekilde hizmet sunmak mümkün olabilmektedir (ENISA, 2006a).

Hizmet verilecek saatler ve ilgili personel konusunda değerlendirilebilecek bir seçenek de diğer STİM'ler ile işbirliği kurmaktır. "Güneşi takip et" ("Follow the Sun") sloganı ile gerçekleştirilen işbirlikleri bulunmaktadır. Bu tarz bir işbirliğinin Avrupa ile Amerika ekipleri arasında yapıldığı ve bu işbirliği ile STİM'lerin

birbirlerinin kapasitelerini kullandıkları ifade edilmektedir. Sun Microsystems firmasına ait STİM'in dünyanın değişik yerlerinde farklı zaman dilimlerinde ofisleri bulunan dağıtık bir yapıda olduğu, bu ekipler arasında sürekli bir görev değişimi yapılarak 7x24 hizmet vermenin başarıldığı dile getirilmektedir (ENISA, 2006a).

b. Gelir modeli

Maliyet modeli ile verilen hizmetlerin getireceği finansal yük belirlenmiş olmaktadır. Bu aşamadan sonra hizmetlerin nasıl finanse edileceği planlanabilmektedir. STİM hizmetlerinin finansmanı konusunda değerlendirilebilecek farklı senaryolar bulunmaktadır (ENISA, 2006a):

- Mevcut kaynakların kullanımı
- Üyelik aidatı ve
- Sübvansiyon.

STİM hizmetlerinin sürdürülebilirliğinin sağlanması STİM'in yeterli fona sahip olması ile mümkündür. Finansmanın sağlanmasında, mevcut kaynakların kullanımı, üyelik aidatı ve sübvansiyon modellerinden biri veya bunların karışımı bir model kullanılabilmektedir (ENISA, 2006a).

1.3.2. Sunulabilecek hizmetler

Bir STİM'in müşterileine sunabileceği çeşitli hizmetler bulunmakla birlikte, bu hizmetlerin kapsamının ve seviyesinin belirlenmesi önem arz etmektedir (ENISA, 2006a).

STİM tarafından sunabilecek çeşitli hizmetlerden bahsetmek mümkündür. Sunulacak hizmetlerin bazıları siber olaylarla mücadele ile doğrudan alakalı iken, güvenlik eğitimleri ve denetimleri gibi bazı hizmetler ise dolaylı olarak alakalıdır (Killcrece vd., 2003a).

Az sayıda ama kaliteli verilen hizmetin çok sayıda fakat kalitesiz verilen hizmetten çok daha yararlı olacağı gerçeğinden hareketle, bir STİM'in her hizmeti vermemesi

kaliteyi arttıracaktır. Sunulacak hizmetler, müşterilerin ihtiyaçları ile yakından alakalıdır ve ihtiyaç analizini yapmak STİM'in sorumluluğundadır (Killcrece vd., 2003a).

Bir STİM tarafından sunulabilecek hizmetler, müşterilerine sunacağı harici hizmetler ve kendi dâhili işlemlerinden oluşmaktadır (ENISA, 2010).

STİM bünyesinde tanımlanmış iç destek süreçlerinin olmasını gerektiren ve genellikle üç sınıfa ayrılan harici hizmetler (ENISA, 2010);

- Herhangi bir siber olay meydana gelmeden müşterinin güvenlik süreçlerini ve altyapısını geliştirmeyi ve böylece siber olay meydana gelse bile etkilerini ve kapsamını asgari düzeyde tutmayı amaçlayan *proaktif hizmetlerden*,
- Müşterilerden STİM'e gelen siber olay ihbarlarına, yardım taleplerine cevap vermeyi ve STİM'in sistemlerini hedef alan tehditlerle mücadeleyi amaçlayan *reaktif hizmetlerden* ve
- Kuruluşun genel güvenliğini arttırmayı amaçlayan *güvenlik kalite yönetimi hizmetlerinden*

oluşmaktadır (Tablo 1.4).

Tablo 1.4. STİM tarafından verilebilecek hizmetler

Reaktif Hizmetler	**Proaktif Hizmetler**	**Güvenlik Kalite Yönetimi Hizmetleri**
•Alarm ve uyarılar • Güvenlik olaylarının ele alınması o Olay analizi o Olaya yerinde müdahale o Olaya müdahale desteği o Olaya müdahale koordinasyonu	• Duyurular • Teknoloji takibi • Güvenlik denetimi veya değerlendirmesi • Güvenlik araçlarının, Uygulamalarının ve altyapıların	• Risk analizi • İş sürekliliği & Felaket kurtarma planları • Güvenlik danışmanlığı • Farkındalık oluşturma • Eğitim, Kurs • Ürün değerlendirme veya belgelendirme

•Güvenlik açıklıklarının ele alınması ○ Açıklık analizi ○ Açıklığa karşılık verme ○ Açıklığa karşılık verme koordinasyonu •Saldırgan araçlarının[2] ele alınması ○ Kodun analizi ○ Koda karşılık verme ○ Koda karşılık verme koordinasyonu	konfigürasyonu ve bakımı • Güvenlik araçlarının geliştirilmesi • Saldırı tespit hizmetleri • Güvenlik ile ilgili bilgilendirme	

Kaynak: (Killcrece vd., 2003a ; ENISA, 2006a)

Reaktif, proaktif ve güvenlik kalite yönetimi hizmetlerinden hangilerinin sunulacağı, STİM'in rolünün belirlenmesinde önem arz etmektedir.

1.3.2.1. Reaktif hizmetler

Reaktif hizmetler STİM'in yürüttüğü faaliyetlerin temel bileşenidir. Bu hizmetler, meydana gelen bir siber olayın bertaraf edilmesini ve bu siber olayın yol açması muhtemel hasarların en az seviyede tutulmasını amaçlamaktadır (ENISA, 2006a), STİM'in müşterilerinin yardım taleplerine veya STİM'in kendi sistemlerini hedef alan tehdit ve saldırılara karşılık vermeyi amaçlamaktadır (Killcrece vd., 2003a).

a. Alarm ve uyarılar

Alarm ve uyarılar, bir saldırı uyarısına, güvenlik açığına veya bilgisayar virüsüne ilişkin açıklayıcı bilgilerin verildiği, bu problemlerle mücadele etmek için çözüm önerileri içeren bir hizmettir. Bu bilgilendirme ile siber olayın hedefi olan

[2] İngilizce artifact olarak adlandırılan kavram, bu çalışmada saldırgan araçları olarak adlandırılmıştır.

müşterilere, sistemlerini korumak veya etkilenen sistemlerini geri kurtarmak için rehberlik sunulmuş olmaktadır (Killcrece vd., 2003a).

Söz konusu hizmet STİM'ler arası iletişimi kapsayabildiği gibi, müşteri kuruluşun sistemlerinde meydana gelen bir siber olaya veya tespit edilen açıklıklara ilişkin de olabilmektedir (ENISA, 2010).

b. Siber olayların ele alınması

Bir siber olayın ele alınması süreci, olaya ilişkin bilgilerin elde edilmesi, olayın önceliklendirmeye tabi tutulması, taleplere cevap verilmesi ve olayın analiz edilmesi aşamalarından oluşmaktadır. Söz konusu süreç (Killcrece vd., 2003a):

- Saldırıdan etkilenen veya tehdide maruz kalan sistemlerin ve ağların korunması için harekete geçmeyi,
- Konu ile ilgili uyarı ve alarmlar ile çözüm ve mücadele stratejileri sağlamayı,
- Saldırının ağın diğer kısımlarındaki faaliyetlerine bakmayı,
- Ağ trafiğini filtrelemeyi,
- Sistemleri ayağa kaldırmayı,
- Sistemleri onarmak veya yamaları yapmayı,
- Diğer müdahale ve geçici çözüm stratejilerini geliştirmeyi

kapsamaktadır.

Siber olaylara karşı koyma yeteneğinin, özellikle uygun kurumsal yapıların oluşturulması ile desteklenmesi gerekmektedir (ENISA, 2010).

Siber olaylar ele alınırken ilk aşamada olayın analiz edilmesi, sonraki aşamalarda olaya yerinde müdahale edilmesi, müdahaleye uzaktan destek verilmesi veya müdahalenin ilgili taraflar arasında koordine edilmesi hizmetlerinden biri veya birkaçının verilmesi söz konusu olabilmektedir (Killcrece vd., 2003a).

b.1. Analiz

Temel olarak olay analizi, bir siber olaya ilişkin mevcut tüm bilgilerin ve delillerin incelenmesi işlemidir. Bu işlem ağın, bilgisayarların ve uygulamaların denetim günlüklerinin, saldırı araçlarının ve kötücül kodların analizini içerebilmektedir. Analizin maksadı, siber olayın kapsamını ve yol açtığı hasarın boyutlarını belirlemek, olayın yapısını anlamak ve muhtemel karşı koyma stratejileri ve çözüm önerilerini ortaya koymaktır (Killcrece vd., 2003a).

b.2. Yerinde müdahale

Siber olayın bertaraf edilmesi ve olumsuz etkilerinin giderilmesi amacıyla STİM müşterilerine olay yerinde destek hizmeti verilebilmektedir. Telefonla veya e-posta ile destek vermek yerine STİM ekipleri olay yerine giderek olaydan etkilenen sistemleri analiz etmekte ve sistemlerin onarılması ve geri kurtarılması faaliyetlerini gerçekleştirmektedir (Killcrece vd., 2003a).

b.3. Müdahale desteği

Siber olayın mağduru olan müşterilere telefon, e-posta, faks veya dokümanlar aracılığıyla rehberlik hizmeti verilmek suretiyle destek sağlanabilmektedir. Bu hizmet kapsamında STİM rehberlik hizmetini uzaktan sunmakta, gerekli önlemler müşteri kurumun/kuruluşun personeli tarafından alınmaktadır (Killcrece vd., 2003a).

b.4. Müdahale koordinasyonu

Bir siber olayın ele alınması sürecinde, saldırının mağduru olan kurum/kuruluş, saldırı ile ilgili olabilecek taraflar arasındaki koordinasyon STİM tarafından sağlanmaktadır. Koordinasyon hizmeti, ihtiyaç duyulan iletişim bilgilerinin toplanması, saldırıya kaynaklık etmesi veya hedef olması muhtemel tarafların uyarılması, olaya muhatap olabilecek taraflara ilişkin istatistiklerin toplanması ve bilgi paylaşımının ve analizinin kolaylaştırılması çalışmalarını içerebilmektedir.

Koordinasyon kolluk kuvvetlerini de kapsayabilen koordinasyon hizmetinde, hiçbir şekilde STİM tarafından olaya yerinde müdahale edilmesi söz konusu değildir (Killcrece vd., 2003a).

c. Güvenlik açıklıklarının ele alınması

Güvenlik açıklıklarının ele alınması hizmeti kapsamında donanım ve yazılımlardaki açıklıklara ilişkin bilgiler ve raporlar değerlendirilmektedir. Söz konusu açıklığın yapısının, bir donanım söz konusu ise mekaniğinin, etkilerinin analiz edilmesi, tespit edilmesi ve onarılmasına yönelik çözüm stratejilerinin geliştirilmesi yapılan çalışmalar arasında yer almaktadır. Güvenlik açıklıkları farklı STİM'ler tarafından farklı şekillerde ele alınmakla birlikte, açıklıkların ele alınmasında aşağıda sıralanan adımlardan bahsetmek mümkündür (Killcrece vd., 2003a).

c.1. Analiz

Açıklık analizi kapsamında, şüphelenilen açıklıkların yerinin ve açıklığın nasıl istismar edilebileceğinin tespit edilmesi amacıyla tetkikler yapılmakta ve donanım veya yazılım teknik olarak incelenmektedir (Killcrece vd., 2003a).

c.2. Karşılık verme

Bir açıklık ile mücadele edilmesi veya açıklığın onarılarak giderilmesi amacıyla karşılık verme yönteminin belirlenmesi işlemidir. Bu işlem ilgili yama, düzeltme ve çözümlerin geliştirilmesini kapsamaktadır. Ayrıca, tavsiye veya uyarılar yayımlamak suretiyle ortaya konan mücadele stratejisi hakkında o an yaşanan siber olayla ilgisi bulunmayan tarafların da bilgilendirilmesi söz konusu olabilmektedir. Üretilen çözümün bir sonucu olarak yama, düzeltme veya diğer çözüm adımlarının uygulanması ile söz konusu güvenlik açıklığına karşılık verilmiş olunmaktadır (Killcrece vd., 2003a).

c.3. Karşılık verme koordinasyonu

Koordinasyon hizmeti ile STİM, müşteri kuruluşun çeşitli birimlerini açıklık konusunda bilgilendirmekte, açıklığın düzeltilmesine ilişkin bilgiler paylaşmaktadır. STİM çözümü, açıklığa karşı koyma stratejisini uyguladıktan ve sonuçların başarılı olduğunu gördükten sonra ilgili taraflarla paylaşmaktadır. Koordinasyon hizmeti kapsamında ihtiyaç duyulması halinde güvenlik üreticileri, diğer STİM'ler, teknik uzmanlar, müşteri kuruluşlar veya açıklığı tespit eden kişi veya gruplarla iletişim kurulmaktadır. Koordinasyon çalışmaları kapsamında, tespit edilen açıklıklara ilişkin bilgilerden ve üretilen çözüm önerilerinde, bir bilgi bankasının oluşturulması da söz konusu olabilmektedir (Killcrece vd., 2003a).

d. Saldırgan araçların ele alınması

Saldırgan araçlar, sisteme yerleşmiş veya yerleştirilmiş, sistemlere ve ağlara yapılan saldırılarda, sızma girişimlerinde veya sistemde alınan güvenlik önlemlerini bertaraf etmede kullanılabilen bir dosya veya nesne olarak tanımlanmaktadır. Saldırgan araçlar, virüsleri, truva atlarını, solucanları, istismar amacıyla yazılmış betikleri ve diğer bazı araçları içerebilmekte ancak bunlarla sınırlı kalmamaktadır (Brown vd., 2003).

Bu hizmet, saldırı girişimlerinde, yetkisiz veya yıkıcı faaliyetlerde kullanılan Saldırgan araçlara ilişkin bilgilerin ve bu araçların birer kopyasının elde edilmesini içermektedir. Söz konusu bilgiler elde edildikten sonra kod(ların) yapısı, mekaniği, sürümü ve kullanımı analiz edilmekte, sonrasında söz konusu kodların tespit edilmesi, sistemden temizlenmesi ve bu kodlara karşı gerekli savunmanın yapılabilmesi amacıyla karşı koyma stratejileri geliştirilmektedir (Killcrece vd., 2003a).

Farklı STİM'ler tarafından farklı şekillerde ele alınmakla birlikte saldırgan araçların incelenmesinde farklı çözüm adımlardan bahsetmek mümkündür.

d.1. Analiz

STİM tarafından yapılan analiz ile, saldırgan araçlara ilişkin elde edilen dosyanın türünün ve yapısının tespit edilmesi, benzerliklerin ve farklılıkların görülmesi amacıyla kodun yeni sürümünün aynı kodun önceki sürümleri ile karşılaştırılması, tersine mühendislik yöntemleri uygulanarak kodun amacının belirlenmesi amaçlanmaktadır (Brown vd., 2003).

d.2. Karşılık verme

Saldırgan araçların tespit edilmesinin ve sistemden temizlenmesinin yanı sıra bu kodların sisteme yüklenmesini ya da girmesini engellemek amacıyla gerçekleştirilecek faaliyetlerin belirlendiği karşılık verme aşamasında, antivirüs yazılımlarına veya saldırı tespit sistemlerine eklenmek üzere saldırgan araçları tanıtan bir imzanın geliştirilmesi hedeflenmektedir (Killcrece vd., 2003a).

d.3. Karşılık verme koordinasyonu

Saldırgan araçlara karşılık verme işleminin koordinasyonu, saldırgan araçların analiz sonuçlarının ve karşılık verme stratejilerinin diğer STİM'ler, araştırmacılar, güvenlik firmaları ve güvenlik uzmanları ile paylaşılması ve sentezlenmesi olarak tanımlanmaktadır. Koordinasyon hizmeti kapsamında bilinen saldırgan araçlardan ve ilgili karşılık verme stratejilerinden bir arşiv de oluşturulabilmektedir. Koordinasyon aşamasının temel hedefi saldırgan araçların yeteneklerinin elde edilmesi ve paylaşılmasıdır (Brown vd., 2003).

1.3.2.2. Proaktif hizmetler

Proaktif hizmetlerin ana hedefi, sistemleri, süreçleri ve personeli daha güvenli hale getiren önleyici tedbirlerin alınması ile siber olayların sayısının azaltılmasıdır. Zira siber olaylarla mücadelenin nihai hedefi olan siber olayların etkilerinin azaltılması ancak olayın meydana geldiği ilk noktada hatta olay meydana gelmeden engellenmesi ile mümkün olabilmektedir (ENISA, 2010).

Farkındalığın arttırılması ve eğitimler düzenlenmesi ile siber olayların meydana gelmesinin önlenmesini amaçlayan proaktif hizmetler ile (ENISA, 2006a), bir siber saldırının meydana gelmesi ihtimaline karşılık müşteri sistemlerinin korunması ve güvenliğinin sağlanması için müşteri kuruluşa bilgi ve destek sağlanmaktadır. Bu hizmetlerin başarılı bir şekilde sunulması, gelecekte müşteriyi etkileyecek siber olayların sayısının azalmasına neden olmaktadır (Killcrece vd., 2003a).

a. Duyurular

Duyuru hizmeti ile saldırı alarmları, güvenlik açığına ilişkin uyarılar ve güvenlik önerileri benzeri konularda müşteri kurumlar/kuruluşlar STİM tarafından bilgilendirilmektedir. Duyurular, yeni tespit edilen güvenlik sorunları istismar edilmeden veya bu sorunların kullanılması ile herhangi bir saldırı gerçekleşmeden müşteri kurumlara/kuruluşlara sistemlerini ve ağlarını korumalarına imkân vermektedir (Killcrece vd., 2003a).

b. Teknoloji takibi

Gelecekte ortaya çıkabilecek tehditlere çözüm üretilebilmesi yeni gelişmelerin, saldırı faaliyetlerinin izlenmesi ve analiz edilmesi ile mümkün olabilmektedir. Takip edilmesi gereken konular ilgili mevzuatı, sosyal veya politik tehditleri gelişmekte olan teknolojileri de kapsayacak şekilde genişletilebilir. Teknoloji takibi hizmetinde STİM, müşterilerin sistemlerinin güvenliğine ilişkin bilgileri elde edebilmek amacıyla güvenlik konularındaki e-posta haberlerini, internet sayfalarını ve yeni yayımlanmış makaleleri takip etmektedir. Bu hizmetin çıktıları arasında çeşitli duyurular, rehberler ya da orta ve uzun vadeli öneriler olabilmektedir. Teknoloji takibi hizmeti esasında güvenlik konusunda bir istihbarat toplama sürecidir (Brown vd., 2003).

c. Güvenlik denetimi veya değerlendirmesi

Organizasyonun kendisi veya standartlar tarafından belirlenen gereksinimler doğrultusunda organizasyonun güvenlik altyapısının detaylı bir şekilde gözden geçirilmesi ve analiz edilmesi sürecidir. Analiz süreci güvenlik işlemlerinin nasıl uygulandığının incelenmesini de kapsayabilmektedir. STİM tarafından sunulabilecek çok farklı denetim veya değerlendirme türleri bulunmaktadır (Killcrece vd., 2003a):

- Altyapının incelenmesi: Organizasyonun güvenlik politikasının ve standartların gereksinimlerinin sağlanıp sağlanmadığının tespit edilmesi amacıyla donanım ve yazılımların, ağ cihazlarının ve sunucuların konfigürasyonlarının elle yapılması,
- En iyi uygulama incelenmesi: Çalışanlar ve ağ ve sistem yöneticileri ile görüşülerek güvenlik uygulamalarının organizasyonun güvenlik politikasına veya standartlara uygunluğunun belirlenmesi,
- Tarama: Açıklık tarama veya virüs tarama araçları kullanılarak hangi sistemin ya da ağın zafiyetinin olduğunun belirlenmesi,
- Penetrasyon testi: Bir birimin sistemlerine ve ağına bilinçli olarak saldırarak o birimin güvenliğinin test edilmesi. Penetrasyon testi sosyal saldırıyı, fiziksel saldırıyı ya da ağ saldırısını kapsayabilmektedir. Kritik bilgilerin ve sunucuların fiziksel güvenliğinin ya da önemli noktalarda çalışan personelin sosyal mühendislik saldırılarına maruz kaldıklarında gizli bilgileri verip vermediklerinin test edilmesi ağ saldırılarına karşı dayanıklılığın test edilmesi kadar önem arz etmektedir.

d. Güvenlik araçlarının, uygulamalarının ve altyapıların konfigürasyonu ve bakımı

Konfigürasyon ve bakım hizmeti ile müşteri kurum/kuruluş ya da STİM'in kendisi tarafından kullanılan güvenlik araçlarının, uygulamalarının ve genel bilgisayar altyapısının güvenli bir şekilde konfigüre edilmesine yönelik rehberlik hizmeti sunulmaktadır. Rehberlik sunmanın yanı sıra STİM, konfigürasyonların ve saldırı tespit sistemi, ağ tarama araçları, güvenlik duvarları veya kimlik doğrulama

mekanizmaları gibi güvenlik araçlarının ve hizmetlerinin güncelleme işlemlerini de gerçekleştirebilmektedir. Bu hizmetlerin dizüstü bilgisayarlar, masaüstü bilgisayarlar ve diğer kablosuz cihazlar için de verilmesi söz konusu olabilmektedir (Killcrece vd., 2003a).

e. Güvenlik araçlarının geliştirilmesi

STİM'in kendisinin veya hizmet verdiği kurumun/kuruluşun ihtiyaç duyduğu bir aracın geliştirmesi söz konusu olabilmektedir. Bu STİM'in müşterileri tarafından kullanılan bir yazılım için veya köle haline getirilmiş bilgisayarların kurtarılması amacıyla kullanılan bir yazılım için yama geliştirilmesini kapsayabilmektedir. Mevcut güvenlik araçlarının yeteneklerinin geliştirilmesi de bu kapsamda değerlendirilmektedir (Brown vd., 2003).

f. Saldırı tespit hizmeti

Bu hizmeti veren bir STİM çalışmalarını, saldırı tespit sisteminin günlük kayıtlarını inceleyerek, belirlenen sınırları aşan olaylar meydana geldiğinde bunları analiz ederek ve ne şekilde karşı koyulacağını göstererek, ya da önceden tanımlanmış servis seviyesi anlaşması çerçevesinde herhangi bir uyarı veya alarm göndererek gerçekleştirmektedir. Saldırı tespit işlemi ve ilgili güvenlik günlük kayıtlarının incelenmesi işlemi yorucu bir süreçtir. Zira bu süreçte sensörlerin konulacağı yerin belirlenmesi ve büyük miktardaki verinin bu yolla elde edilmesi ve incelenmesi zorlu bir aşama olarak STİM'lerin karşısına çıkmaktadır. Bu faaliyetler bazı organizasyonlar tarafından hizmet alımı yoluyla gerçekleştirilmektedir (Killcrece vd., 2003a).

g. Güvenlik konularında bilgilendirme

Bu hizmetle müşterilere güvenliği arttırmada yardımcı olacak kapsamlı bilgiler sağlanmaktadır. Sağlanan bilgiler;

- Rehberlik ve STİM iletişim bilgilerinin raporlanmasını,
- Yapılan alarmların, uyarıların ve duyuruların arşivlerini,
- Mevcut durumdaki en iyi uygulamaya ilişkin dokümanı,
- Genel bilgisayar güvenliği konusunda rehberliği,
- Politikaları ve süreçleri,
- Yama geliştirilmesini ve bilgi dağıtımını,
- Ürün satıcılarının bağlantı adreslerini,
- Güvenlik olayı raporlarının gidişatı ve mevcut istatistiklerini

içerebilmektedir (Brown vd., 2003).

1.3.2.3. Güvenlik kalite yönetimi hizmetleri

Güvenlik kalite yönetimi hizmetleri, siber olayların ele alınmasından bağımsız olarak, kuruluşun bilgi teknolojileri, denetim ve eğitim birimleri tarafından sunulan hizmetlerin hem sayı olarak çoğalmasına hem de kalitesinin artmasına katkı sağlamaktadır. Müşteri kuruluş tarafından mevcutta sunulan hizmetlerin STİM tarafından verilmeye başlanması veya bu hizmetlerin sunulması konusunda STİM'den destek alınması, kuruluşun güvenlik seviyesini arttıracaktır. Güvenlik kalite yönetimi hizmetleri genel olarak proaktif hizmetler sınıfında kabul edilmekte ve siber olayların azalmasına dolaylı olarak katkı sağlamaktadır (Killcrece vd., 2003a). Güvenlik konusunda farkındalık oluşturma, iş sürekliliği veya risk analizi gibi hizmetler güvenlik kalite yönetimi kapsamında sunulabilecek hizmetler arasında yer almaktadır (ENISA, 2010).

Kalite yönetimi hizmetleri ile yukarıda bahsedilen reaktif ve proaktif hizmetlerin verilmesinden kazanılan deneyimler doğrultusunda, bir STİM'in güvenlik anlayışına başka yollarla elde edilemeyecek farklı bir bakış açısı getirmesi beklenmektedir (Killcrece vd., 2003a).

a. Risk Analizi

Risk analizi ve değerlendirme sürecine STİM'in katacağı değerin, gerçek tehditlerin değerlendirilmesine, bilgi varlıklarına yönelik risklerin daha gerçekçi bir şekilde nitel ve nicel olarak değerlendirilmesine ve sonucunda ise koruma ve karşı koyma stratejilerini daha da geliştirmeye katkı sağlayacağını söylemek mümkündür. Bu hizmeti veren STİM'lerin yeni sistemlere ilişkin bilgi güvenliği risk analizi veya müşterinin sistemlerini hedef alan yeni tehditler ve saldırılar konusunda çalışmalarına katılarak katkı sağlamaları gerekmektedir (Brown vd., 2003).

b. İş sürekliliği & Felaket kurtarma planları

Güvenlik olaylarının veya güvenlik eğilimlerinin geçmişteki durumuna ve gelecekteki durumlarına ilişkin yapılan tahminlere bakılarak, çok sayıda güvenlik olayının işletmelerin faaliyetlerini önemli ölçüde bozma potansiyeline sahip oldukları ifade edilmektedir. Bu nedenle iş sürekliliğinin sağlanması amacıyla bu tür güvenlik olaylarına en iyi nasıl karşı koyulacağının belirlenmesi aşamalarında STİM'in deneyimlerinin ve tavsiyelerinin hesaba katılması gerekmektedir. Bu hizmeti sunan STİM'lerin iş sürekliliği ve felaket kurtarma planları konularında da çalışmaları gerekmektedir (Killcrece vd., 2003a).

c. Güvenlik danışmanlığı

STİM, müşteri kurumun/kuruluşun işletme faaliyetleri için en iyi güvenlik uygulamalarının sağlanması konusunda rehberlik ve tavsiyeler sunabilmektedir. Güvenlik danışmanlığı hizmetini sunan bir STİM'in, tavsiye hazırlama, yeni sistemlerin, ağ cihazlarının ve yazılım uygulamalarının satın alınması, yüklenmesi ve güvenliğinin sağlanması konuları ile ilgilenmesi gerekmektedir (Killcrece vd., 2003a).

d. Farkındalık oluşturma

Makul güvenlik uygulamaları ve güvenlik politikaları konularında müşterinin hangi noktalarda rehberliğe ve bilgiye gereksinim duyduğunun STİM tarafından belirlenmesi önem arz etmektedir. Müşterinin çalışanlarının güvenlik konusundaki farkındalıklarının arttırılması, güvenlik sorunlarının anlaşılması yeteneğini geliştirmekte ve günlük yürütülen faaliyetlerin daha güvenli bir şekilde gerçekleştirilmesine katkı sağlamaktadır. Bu gelişimin başarılı saldırıların sayısını azaltabileceğini, saldırıların ve tehditlerin organizasyon tarafından tespit edilme ihtimalini arttırabileceğini beklemek mümkündür. Dolayısıyla bunun da geri kurtarma sürelerini azaltacağı ve kayıpları ortadan kaldıracağı öngörülmektedir (Brown vd., 2003).

e. Eğitim/Kurs

Eğitim ve kurs hizmeti ile seminer, çalıştay ve kurslar düzenleyerek müşteriye siber olaylar hakkında bilgi verilmesi amaçlanmaktadır. Konu başlıkları, bir güvenlik olayının raporlanması, uygun karşı koyma yöntemleri, karşı koyma araçları, siber olayı önleme yöntemleri ve siber olaylara ilişkin koruma, tespit, raporlama ve karşı koymaya ilişkin gerekli diğer bilgiler şeklinde olabilmektedir. Hizmet kapsamında belirli bazı siber olaylara, açıklıklara veya sosyal mühendislik konularına yönelik kurslar da düzenlenebilmektedir (Brown vd., 2003).

f. Ürün değerlendirme ve belgelendirme

Bu hizmet kapsamında STİM, kullanılan araçları, uygulamaları ve ürünlerin güvenliğini ve organizasyonun güvenlik uygulamalarına uygunluğunu sağlamak üzere sunulan diğer hizmetleri değerlendirmeye tabi tutabilmektedir. Bu kapsamda hem açık kaynak kodlu ürünler hem de ticari ürünler incelenebilmektedir. Değerlendirme ve belgelendirme hizmeti bir sertifika programı aracılığıyla verilebilmektedir (Killcrece vd., 2003a).

1.3.2.4. U-STİM tarafından sunluacak asgari hizmetler

Bir güvenlik organizasyonunun STİM olabilmesi için, bu bölümde bahsi geçen hizmetlerin uygun bir alt kümesi ile hizmet vermeye başlaması önerilmektedir. Söz konusu küme belirlenirken, sahip olunan mevcut kaynakların ve personelin göz önünde bulundurularak gerçekten sunabilecek hizmetlerin seçilmesi önem arz etmektedir. Söz konusu alt kümede siber olaylara müdahale hizmetinin muhakkak yer alması gerekmektedir. Kalite odaklı hizmet ile müşterilerin güveninin kazanılmasını müteakip ihtiyaç duyuldukça verilen hizmet sayısının arttırılmasının daha etkili olacağı değerlendirilmektedir (Brown vd., 2003).

Başlangıçta verilebilecek hizmetlerin yaklaşık olarak hangileri olduğu noktasında genel bir mutabakatın ortaya çıktığını söylemek mümkündür. Bu hizmetlerin, son on yılda STİM/KM ve diğer ekiplerin güvenlik olaylarına karşı koyma faaliyetlerinden edinilen ortak tecrübeler ve bilgiler ve diğer STİM'ler ile yapılan tartışmalar, literatürün incelenmesi ve bazı STİM'lerin tesislerinde yapılan araştırmalar neticesinde belirlendiği ifade edilmektedir (Killcrece vd., 2003a).

Temel kümede yer alan hizmetlerin STİM'ler tarafından yaygın bir şekilde sunulan hizmetler olduğu görülmektedir. Listedeki her hizmetin sunulması zorunlu olmamakla birlikte birçok güvenlik ekibi listede yer alan hizmetlerin birini veya birkaçını sunmaktadır. Dolayısıyla bu listenin hizmet vermeye yeni başlayacak ekiplere bir fikir vereceği düşünülmektedir (Killcrece vd., 2003a).

Temel kümede yer alan hizmetler:

- Reaktif hizmetler
    - Alarm ve uyarılar,
    - Güvenlik olaylarının ele alınması,
        - Olay analizi ve olaya yerinde müdahale, olaya müdahale desteği ve olaya müdahale koordinasyonundan en az biri,
    - Güvenlik açıklıklarının ele alınması,
        - Açıklığa karşı koyma koordinasyonu,

- Proaktif hizmetler
    - Duyurular,
- Güvenlik kalite yönetimi hizmetleri
    - Farkındalık oluşturma,
    - Güvenlik danışmanlığı özellikle güvenlik politikası geliştirme

sayılmaktadır (Killcrece vd., 2003a).

STİM'in vermesi gerekli olan hizmetlerin başında olay yönetimi ve açıklık yönetimi gelmektedir. Ulusal bir STİM'in hizmetlerini sunabilmesi ancak uygun ve yeterli sayıda personele, teknolojik altyapıya ve iyi tanımlanmış iş süreçlerine sahip olması ile mümkündür. Bu yeteneklere sahip olmayan bir STİM'den verilmesi gereken asgari hizmetleri vermesi dahi beklenememektedir (ENISA, 2010).

Ulusal bir STİM'in müşterilerine yeterli kalitede hizmet verebilmesi için sahip olması gereken yetenekler;

- Yeterli insan kaynağı,
- Bina, ağ ve bütçe gibi bileşenlerden oluşan altyapı,
- Hizmet sunumu ve
- İş sürekliliği

olarak sayılmaktadır (ENISA, 2010).

Ulusal bir STİM'in en temel rolünün ulusal bilgi altyapılarını etkileyen bir krizde koordinasyonu sağlamak olmasından dolayı her koşulda hizmet vermeye devam edebiliyor olması gerekmektedir. Bundan dolayı STİM için iş sürekliliği büyük önem arz etmektedir.

Belirlenen başlangıç hizmetler ile faaliyetine başlayan STİM'in sürdürülebilir bir yapı ile çalıştırılması hem hizmeti sunan taraf olarak STİM için hem de hizmeti alan taraflar olarak müşteriler için kritik bir önem arz etmektedir. Zira güvenlik olaylarının önlenmesi, etkilerinin en aza indirilmesi ve oluşabilecek hasarların en kısa sürede giderilmesi süreklilik arz etmesi gereken hizmetlerdir. Siber olaylara

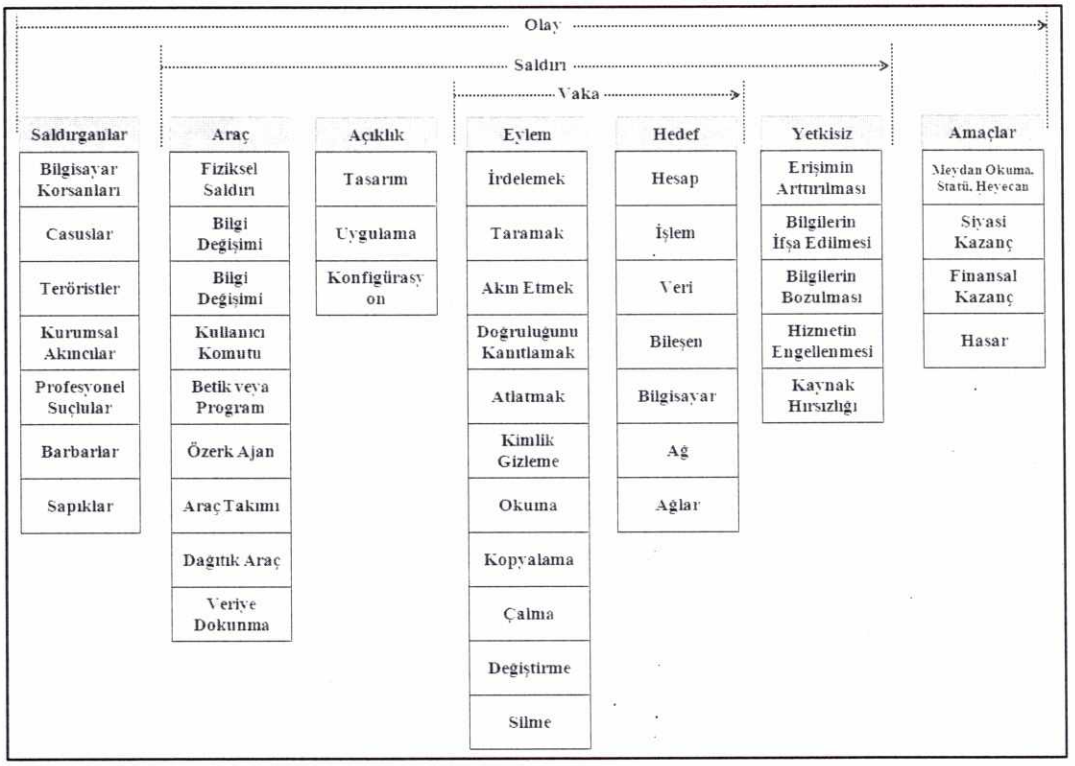
müdahale faaliyetlerinde sürekliliği sağlamak ancak siber olayların ve güvenlik açıklarının etkin bir şekilde ele alınması ile mümkün olabilmektedir.

1.3.3. Siber Olayların ve Açıklıkların Yönetimi

Siber olayların yönetimi acil sağlık hizmetlerine benzetilmektedir. Olayla ilgilenen kişinin baskı altında olma eğiliminde olması çok pahalıya mal olabilecek hataların yapılmasına yol açabilmektedir. Böyle durumlarda basit ve iyi anlaşılmış bir yolun denenmesinin en iyi sonucu vereceğine inanılmaktadır. Bu nedenledir ki siber olayların ele alınması konusunda en deneyimli uzmanlar dahi, siber olaylara karşı koyarken iyi tanımlanmış ve sistematik prosedürleri takip etmekte, siber olayın ele alınmasının altı aşaması olan hazırlık, tespit, kuşatma, yok etme, kurtarma ve olay sonrası faaliyetler adımlarını dikkate almakta ve bu adımlara ilişkin önceden hazırlanmış yöntemleri kullanmakta ve gerekli olan durumlarda başkalarından yardım da isteyebilmektedir (Northcutt, 2003).

Bilgisayar veya ağlara yapılan saldırılar genellikle kendine özgü bir grup halinde meydana gelmekte ve bu saldırılar bir siber olayın parçası olarak değerlendirilmektedir. Bu saldırıları kendine özgü bir grup yapan ve hakkında kısmi bilgiye sahip olunan bir dizi faktör bulunmaktadır. Örneğin bir saldırının arkasında sadece bir saldırganın veya birbiriyle bir şekilde ilişkili birden fazla saldırganın olması, saldırganın hedefine karşı benzer saldırıları kullanması, saldırganların benzer veya farklı hedefler için çalışması, saldırıların hedefinin ve zamanlamasının aynı olması bu faktörlerden arasında sayılmaktadır. Dolayısıyla siber olayı, saldırganların, saldırıların, amaçların, seçilen hedeflerin ve zamanlamanın farklı olmasıyla diğer saldırılardan ayırt edilebilen saldırılar kümesi olarak tanımlamak mümkündür (Howard ve Longstaff, 1998). Bir diğer deyişle saldırganların aynı veya ilişkili, saldırıların aynı veya benzer, amaçların ortak, seçilen hedeflerin ilişkili ve zamanlamanın aynı olduğu saldırlar kümesi bir siber olaya karşılık gelebilmektedir. Siber olay, siber saldırı ve vaka arasındaki farklılıklar Şekil 1.8'de görülmektedir.

Şekil 1.8. Siber olayların sınıflandırılması



Kaynak: (Howard ve Longstaff, 1998)

STİM dünyasında STİM tarafından yürütülen faaliyetlerin bir kısmı *olaya karşı koyma* ve *olayı ele alma* kavramları ile ifade edilmektedir. STİM sadece bu faaliyetleri yürütmemekte, olaya karşı koyma ve olayın ele alınması dışında da çeşitli faaliyetler yürütmektedir. Bu geniş faaliyet kümesini ifade etmek için ise *olay yönetimi* ifadesi kullanılmaktadır. Dolayısıyla olaya karşı koyma, olayı ele alma ve olay yönetimi arasında hem kapsam hem de seviye olarak çeşitli farklılıkların olduğunu söylemek mümkündür (Alberts vd. , 2004).

Olayın ele alınması, bir olayın ele alınması sürecindeki tüm süreçleri içeren hizmeti ifade etmektedir. Olayın ele alınması birden fazla işlevi içermektedir (Alberts vd. , 2004):

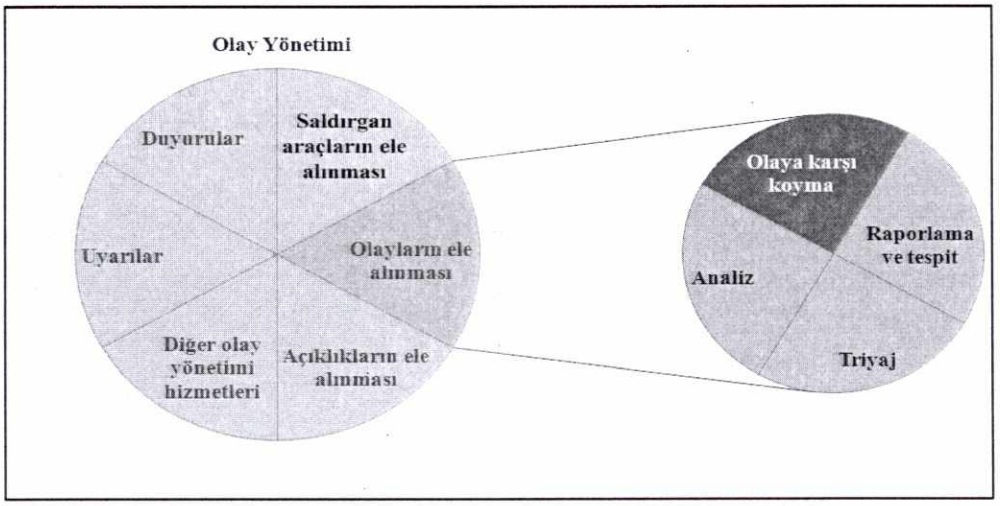
- Tespit ve raporlama: Olay bilgilerinin, olay raporlarının ve alarmların alınıp işlenmesi yeteneğidir.
- Triyaj: Olayların kategorize edilmesi, önceliklendirilmesi için yapılan işlemdir.

- Analiz: Neyin meydana geldiğinin, etkisinin ve zararının ne olduğunun, hangi kurtarma ve azaltma adımlarının atılacağının değerlendirilmesidir.
- Olaya karşı koyma: Bir olayın bertaraf edilmesi, bilgilerin koordine edilmesi ve taraflara ulaştırılması için ve olayın yeniden meydana gelmesini önlemek amacıyla atılan adımları ifade etmektedir.

Dolayısıyla olaya karşı koymanın olayı ele alma sürecinin son adımı olduğu görülmektedir (Alberts vd. , 2004).

Olay yönetimi kavramı ise, STİM tarafından olayların ele alınması dışında yürütülen açıklıkların ele alınması, saldırgan araçların ele alınması, güvenlik farkındalık eğitimleri gibi faaliyetleri kapsamaktadır (Şekil 1.9). Dolayısıyla olay yönetimi sadece bir olayın meydana gelmesi durumunda yapılan müdahale ile sınırlı kalmamakta, siber tehditlere ve risklere karşı yürütülen proaktif faaliyetleri de içermektedir (Alberts vd. , 2004).

Şekil 1.9. Olayın yönetimi, ele alınması ve olaya karşı koyma arasındaki ilişki



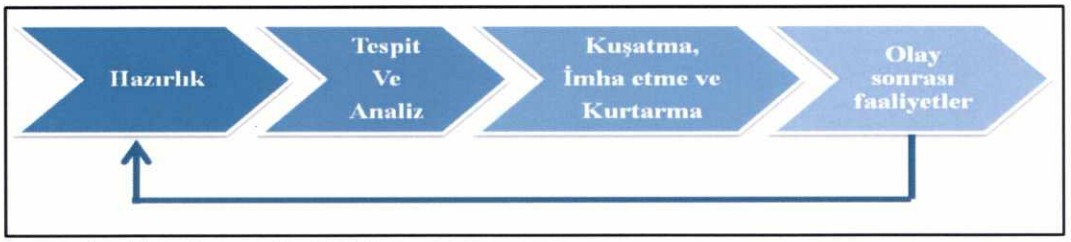
Kaynak: (Alberts vd. , 2004)

1.3.3.1. Siber olayların ele alınması aşamaları

Siber olaya karşı koyma sürecinin temel adımları farklı kaynaklarda farklı şekilde ele alınmaktadır. Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of

Standards and Technology - NIST) siber olayların ele alınmasını Şekil 1.10'da gösterildiği gibi hazırlık çalışmaları, tespit ve analiz aşaması, kuşatma-imha etme ve kurtarma aşaması ve olay sonrası analizler olmak üzere dört temel adımda göstermektedir (Scarfone vd., 2008). Sistem yöneticisi, Denetim, Ağ ve Güvenlik enstitüsü (SysAdmin, Audit, Network, Security - SANS) ise bu aşamaları hazırlık, tespit, kuşatma, yok etme, kurtarma ve olay sonrası faaliyetler şeklinde altı adımda ele almaktadır (Northcutt, 2003).

Şekil 1.10. Siber olaylara müdahale adımları



Kaynak: (Scarfone vd., 2008).

İlgili organizasyonu siber olay konusunda uyarmak için meydana gelen güvenlik ihlalinin tespit edilmesi gerekmektedir. Tespit edilen siber olayın etkilerini azaltmak ve olayı bertaraf etmek amacıyla harekete geçilmelidir. Olaya gerekli ölçüde müdahale edildikten sonra olayın nedenini, maliyetini ve benzer olayların gelecekte yaşanmaması için alınması gereken önlemleri konu alan bir rapor hazırlanmaktadır (Scarfone vd., 2008).

a. Hazırlık aşaması

Hazırlık aşaması, siber olaylara müdahale faaliyetlerini yürütecek bir ekibin kurulması, bu ekibin eğitilerek ihtiyaç duyulan uzmanlık seviyesine ulaştırılması ve gerekli araçların ve kaynakların bu ekibe sağlanması çalışmalarından oluşmaktadır. Ayrıca risk değerlendirme sürecinin bir çıktısı olarak alınan çeşitli kararların uygulanması ile meydana gelebilecek siber olayların sayısının azaltılmasının hedeflenmesi de hazırlık aşamasında yürütülen çalışmalar arasında yer almaktadır (Scarfone vd., 2008).

Benzer şekilde SANS da hazırlık aşamasında yapılabilecek çalışmalar arasında proaktif teknikler kullanılarak olayın önlenmesini, olayın ele alınması yeteneğinin desteklenmesi için yönetim desteğinin sağlanmasını, olayı ele alacak personelin belirlenmesini ve takımın organize edilmesini, bir acil durum iletişim planının geliştirilmesini, takım üyeleri için kursların düzenlenmesini, organizasyondaki bölümler arasında işbirliğinin sağlanması için ilkelerin belirlenmesini, kolluk birimleri ve diğer STİM'lerle arayüzler geliştirilmesini saymaktadır (Northcutt, 2003).

Siber olaylara müdahale yöntemlerinde hazırlık aşamasının, sadece olaylara müdahale yeteneğinin oluşturulmasını değil aynı zamanda sistemlerin, ağın ve uygulamaların yeterince güvenli olmalarını sağlayarak siber olayların önlenebilmesini kapsaması gerektiği değerlendirilmektedir. Siber olaylara müdahale ekibinin siber olayların meydana gelmesinin önlenmesi gibi ana bir sorumluluğu olmamasına karşın, böyle bir ekip tarafından yapılacak tavsiyelerin sistemlerin güvenliğinin sağlanması ve dolayısıyla da siber olayların önlenmesine katkı sağlayacağına inanılmaktadır (Scarfone vd., 2008).

Siber olayların ele alınmasının ilk adımı olan hazırlık aşaması, olaya müdahale hazırlığı, olayın önlenmesine ilişkin çalışmalar ve yönetimin desteğinin sağlanması gibi faaliyetlerden oluşmaktadır.

a.1 Olaya müdahale hazırlığı

Siber olaylara müdahale süreci çeşitli bilgi teknolojileri araçlarına, işbirliği kapsamında diğer güvenlik ekiplerine, yararlı bilgilerin yer aldığı internet sayfası adreslerine ihtiyaç duyulabilecek bir süreçtir (Tablo 1.5). Hazırlık aşamasında bu bilgilerin olaya müdahale edecek personelin kullanabileceği şekilde derlenmiş olması gerekmektedir (Scarfone vd., 2008).

Tablo 1.5. Siber olaylara müdahale personeli için araçlar ve kaynaklar

Araç / Kaynak	Açıklama
Olaylara müdahale personelinin iletişimi ve araçları	Ekip üyelerinin ve kolluk birimlerinin ve diğer STİM'lerin birincil ve yedek kontak bilgileri, iletişime geçilecek kişinin kimliğinin doğrulanması adımları
	Organizasyondaki nöbetçi ekiplerin iletişim bilgileri.
	Kullanıcıların şüpheli olayları bildirebilecekleri telefon numarası, elektronik posta adresi ve çevrim içi formlar gibi olay raporlama mekanizmaları. Bu mekanizmalardan en az bir tanesinin olayları anonim olarak ihbar etmeye imkân vermesi.
	Çalışma saatleri dışında destek vermeleri amacıyla ekip üyelerinin yanlarında cep telefonu veya çağrı cihazı taşımaları.
	Ekip üyeleri arasındaki ve dış birimlerle olan iletişimi şifreleyecek bir şifreleme yazılımı. Yazılımın onaylanmış bir algoritma kullanması.
	Merkezi iletişim ve koordinasyon için kalıcı veya ihtiyaca göre oluşturulacak bir komuta merkezi.
	Deliller ve diğer hassas bilgiler için güvenli bir saklama alanı.
Olay analiz donanımı ve yazılımı	Disk görüntüleri almak, günlük dosyalarını ve olayla ilgili diğer verileri korumak için adli bilişim iş istasyonları ve yedekleme cihazları.
	Dizüstü bilgisayarlar
	Yedeklerin geri yüklenmesi, kötücül kodların denenmesi gibi çeşitli amaçlarla kullanılabilecek yedek iş istasyonları, sunucular ve ağ cihazları. Sanal laboratuar kurma yeteneği sunan yazılımlar.
	Sarf malzemeleri.
	Ağ trafiğinin analiz edilmesi için paket izleme ve protokol analiz programları
	Disk görüntülerinin analiz edilmesi için adli bilişim yazılımı.
	Sistemlerden delil elde edebilecek güvenilir programlar içeren taşınabilir diskler
	Muhtemel yasal işlemler için delilleri korumak amacıyla sayısal kameralar, ses kaydediciler, delil saklama çantaları ve bantları gibi delil toplama araçları.
Olay analiz kaynakları	Sık kullanılan ve Truva atlarının kullandığı portların listesi.
	İşletim sistemleri, uygulamalar, protokoller ve saldırı tespit sistemlerine ilişkin dokümanlar ve antivirüs imzaları.
	Ağ diyagramları ve kritik varlıkların listesi.
	Olayın analizini, doğrulanmasını ve imha edilmesini hızlandırmak için kritik dosyaların şifreli özetleri
Siber olayları önleme yazılımları	İşletim sistemi ön yükleme diskleri ve uygulama programları diskleri
	İşletim sistemi ve uygulama yazılımı satıcılarının güvenlik yamaları
	İşletim sisteminin, uygulamaların ve ikincil alanlara yedeklenen verinin görüntüsünün yedeği.

Kaynak: (Scarfone vd., 2008)

a.2 Yönetim desteğinin sağlanması

Yönetimin desteği alınmadan, siber olayların ele alınmasına dolayısıyla da önlenmesine vakit ve para ayırma, politik destek sağlama konusunda zorluklar yaşanmaktadır. Söz konusu desteğin alınması için:

- Resmi ve yazılı bir siber olaylara karşı koyma planının oluşturulması,
- Siber olayların görsel grafik olarak gösterilmesi,
- Geçmişte karşı koyulan siber olaylara ve bu karşı koymanın kazandırdıklarına ilişkin bilgilerin sunulması ve
- Olaylara karşı koymada karar almanın kritik öneminden dolayı, müdahale ekibinin gerekli ve yeterli yetkiye sahip olması

sağlanmalıdır (Northcutt, 2003).

a.3 Olayın önlenmesine yönelik çalışmalar

Bir siber olayın en etkin bir şekilde ele alınmasının yolu, olayın ilk meydana geldiği yerde durdurulmasıdır. Bunun yapılabilmesi için, bir güvenlik politikasının olmasına, ağ trafiğinin izlenmesi ve analiz edilmesine, bir güvenlik açığı yama programının uygulanmasına, açıklıkların değerlendirilmesine, ilgili personelin teknik yeteneklerinin geliştirilmesine, sistemlerin dikkatlice yapılandırılmasına ve siber olayların ele alınmasına ilişkin bir eğitim programının oluşturulmasına ihtiyaç duyulmaktadır (Northcutt, 2003).

Siber olayların sayısının makul bir seviyede tutulması bir organizasyonun korunmasında büyük önem taşımaktadır. Güvenlik denetimlerinin yetersiz olması, STİM'in mevcut kapasitesini aşacak kadar çok sayıda siber olayın meydana gelmesi ihtimalini arttırmaktadır. Bu ihtimal olaylara yavaş ve eksik cevap verilmesi sonucunu doğurabilmektedir. Bu sonuç ise beraberinde daha büyük hasarların oluşması, hizmetlere veya verilere ulaşılamaması gibi olumsuz başka sonuçlara yol açabilmektedir. Bu durumun önüne geçebilmek için, periyodik olarak sistemleri ve uygulamaları risk değerlendirmesine tabi tutarak, hangi açıklıkların hangi tehditlere davetiye çıkardığının belirlenmesi, risklerin önceliklendirilmesi ve uygun çözümlerin geliştirilmesi gerekmektedir. Gün geçtikçe yeni tehditler ve açıklıkların ortaya çıkmasından hareketle risk değerlendirmesinin makul aralıklarla tekrarlanmasında yarar görülmektedir (Scarfone vd., 2008).

Risk değerlendirmesi ile ayrıca, kritik kaynaklar belirlenmiş olmakta, STİM çalışanlarının belirlenen bu kaynakları öncelikli olarak izlemelerine ve muhtemel bir

saldırıda söz konusu kaynakları nasıl koruyacaklarına ilişkin çalışmalar yapmalarına da imkân sağlanmaktadır (Scarfone vd., 2008).

Sistem ve ağ güvenliğinin sağlanması konusunda, yamaların takip edilmesi, kullanıcı bilgisayarlarının ve sunucuların güvenliğinin sağlanması, kötücül kodlarla mücadele edilmesi ve kullanıcı farkındalığının arttırılması çalışmalarının yürütülmesinin yararlı olacağı düşünülmektedir (Scarfone vd., 2008).

a.4 Olayı ele alacak personelin belirlenmesi ve takımın organize edilmesi

Siber olayların ele alınması işi tek kişilik bir iş değil bir takım işidir. Dolayısıyla takım oluşturulurken doğru personelin seçilmesi, personelin doğru hazırlık çalışmaları ile doğru yerde çalıştırılması STİM'in verimini arttıracaktır. Bunun sağlanabilmesi amacıyla;

- Takıma katmak üzere nitelikli personelin seçilmesi,
- Yerel, merkezi veya ikisinin karışımı bir takım modelinin seçilmesi,
- Organizasyonun halkla ilişkiler bölümünde görev alacak doğru personelin seçilmesi,
- Organizasyonun felaket kurtarma planının siber olayların ele alınmasını içerecek şekilde güncellenmesi,
- Personel için tazminat planlarının oluşturulması ve
- Ağ diyagramlarının ve kontrol listelerinin oluşturulması

önerilmektedir (Northcutt, 2003).

a.5 Acil durum iletişim planı geliştirilmesi

İletişimin sağlanması ve ilgili personelin bilgilendirilmesi genellikle iyi anlaşılan temel görevlerdendir. Ancak siber olay esnasında beklenmedik yeni bir vaka ile karşılaşılması durumunda doğal iletişim kanalları çalışmamaktadır. Bu beklenmedik durumun aşılması amacıyla;

- Bir arama listesi oluşturulması ve kişilerin hızlı bir şekilde bilgilendirilmesi için yöntemler geliştirilmesi,

- Siber olay uyarı arama ağacı oluşturulması,
- Arama ağacının bir yedeğinin kuruluşun bulunduğu yerin dışında bir yerde arama listesi ve tutulması,
- Parolaların ve şifreleme anahtarlarının güncelliğinin ve erişilebilirliğinin sağlanması,
- Birincil bir irtibat noktasının ve siber olay komuta ve iletişim merkezinin oluşturulması,
- Çok kritik durumlarda güvenli iletişimin kurulması,
- Personelin siber olaya müdahale ederken ihtiyaç duyabileceği kaynakları edinme planının oluşturulması

gerekmektedir (Northcutt, 2003).

a.6 Kolluk birimleri ve diğer STİM'lerle arayüz geliştirilmesi

Önceden kurulmuş ilişkilerin olması durumunda, acil yardımca ihtiyaç duyulduğunda yardım çok daha kolay elde edilecektir. Siber olayların ele alınması konusunda birden faza kolluk biriminin olması ve bu birimlerin görev alanlarının örtüşmesi söz konusu olabilmektedir. Bu durumda karşılaşılan zorluk siber olay hakkında bilgisi olan kişilerin bulunması ve iletişime geçilmesidir. Söz konusu zorluğun aşılması veya yaşanmaması için;

- Siber olaylara ilişkin yürürlükte olan mevzuatın bilinmesinin,
- Kolluk birimlerini ilgilendirecek durumların bilinmesinin ve
- Bir siber olay meydana gelmeden önce yerel kolluk birimleri ile iletişime geçilmesinin

yararlı olacağı değerlendirilmektedir (Northcutt, 2003).

b. Tespit ve analiz aşaması

Tespit aşamasında bir siber olayın meydana geldiğinin belirlenmesi, meydana geldiği durumda ise yapısının belirlenmesi amaçlanmaktadır. Tespit aşaması sistemde veya ağda sıra dışı bir durumun farkına varılmasının ardından başlamaktadır. Bu aşama aynı zamanda, sorunun aşılması için yardım alınabilecek kişilere konu hakkında bilgi

verilmesini ve yardım talep edilmesini de kapsamaktadır. Tespit aşamasında dikkat edilmesi gereken önemli bir nokta olarak, sistemlerde meydana gelen her sıra dışı durumun bir siber olayın habercisi olmayabileceğinin altı çizilmektedir (Northcutt, 2003).

Bir siber olayın tespit edilmesi aşaması, siber olayın kategorisinin belirlenmesi, siber olaya ilişkin belirtilerin ve bu belirtilerin kaynaklarının bilinmesi, olayın analiz edilmesi ve bilgi bankasına eklenmek üzere belgelendirilmesi adımlarından oluşmaktadır.

b.1 Siber olayla ilgilenecek bir personelin belirlenmesi

Merkezi bir kontrol noktası olmadığı zaman birçok kişinin farklı amaçlar için çalışması söz konusu olabilmektedir. Yönlendirilmeyen çalışmalar yanlış sonuçların elde edilmesine, delillerin kaybolmasına ve siber olayın yol açacağı durumdan daha kötü durumların oluşmasına yol açabilmektedir. Bu durumun önüne geçilmesi amacıyla;

- Tespiti ve değerlendirmeyi yönetecek ve koordine edecek personelin belirlenmesi ve
- Siber olaya ilişkin günlük kaydının tutulması

gerekmektedir (Northcutt, 2003).

b.2 Siber olay kategorileri

Dinamik doğası gereği siber olaylar sayısız şekillerde meydana gelebilmektedir. Dolayısıyla her olaya müdahale için ayrı bir sürecin tanımlanması mümkün değildir. Bu noktada her siber olay için bir genel müdahale sürecinin, yaygın siber olaylar için ise özel müdahale süreçlerinin belirlenmesi benimsenmektedir (Tablo 1.6).

Tablo 1.6. Siber olay kategorileri

Olay	Açıklama
Hizmeti durdurma (DoS)	Kaynakları tüketerek ağın, sistemin veya uygulamanın yetkili bir şekilde kullanılmasını engelleyen siber saldırı.
Kötücül kod	Bir bilgisayara bulaşabilen bir virüs, Truva atı veya başka kötücül bir kod.
Yetkisiz erişim	Bir kişinin bir ağa, sisteme, uygulamaya, veriye veya diğer Bilgi teknolojisi kaynaklarına mantıksal veya fiziksel izinsiz erişim elde etmesi.
Kötüye kullanım	Bir ağın veya güvenlik politikasının kabul edilebilir kullanımının bir kişi tarafından ihlal edilmesi.
Çoklu bileşen	İki veya daha fazla siber olayı kapsayan siber olay.

Kaynak: (Scarfone vd., 2008)

b.3 Siber olayın belirtileri

Bir siber olayın meydana geldiğinin tespit edilmesi, meydana gelmiş ise olayın türünün, kapsamının ve büyüklüğünün belirlenmesi uzmanlık gerektirmektedir. Bu sürecin zorlu kılan faktörler arasında (Scarfone vd., 2008):

- Siber olayların çok farklı detaylara sahip olabilmelerinden dolayı çok farklı yollarla tespit edilmeleri,
- Muhtemel siber olayların belirtilerinin sayısının bir hayli yüksek olması ve
- Siber olaylara ilişkin verileri doğru ve etkin bir şekilde analiz edilebilmek için detaylı ve uzman düzeyde teknik bilgiye ve deneyime ihtiyaç duyulması

sıralanmaktadır.

Siber olaya ilişkin bir belirti, meydana gelmiş ya da o anda meydana gelmekte olan bir olayın bulgusu (ardıl belirti) veya gelecekte meydana gelmesi muhtemel bir olayın habercisi (öncül belirti) olabilmektedir. Ardıl belirtilere (Scarfone vd., 2008):

- Bir bilgisayara bir solucanın bulaşması durumunda antivirüs programının uyarması,

- İnternet sayfasının çökmesi,
- Dosya adının sıra dışı karakterlerden oluştuğu bir dosyaya rastlanması,
- Bir uygulamaya ait günlük kayıtlarında yabancı bir sistemden çok sayıda oturum açma girişiminin olduğuna ilişkin kayıtlara rastlanması

Öncül belirtilere ise:

- İnternet sayfasının yayın yaptığı sunucunun günlük kayıtlarında açıklıkların tarandığına ilişkin kayıtların olması,
- Elektronik posta sunucusunun bir açıklığını hedef alan bir tehdide ilişkin bir duyurunun yayımlanması veya
- Saldırı düzenleneceğine ilişkin korsan grubundan bir tehdidin alınması

örnek verilebilir (Scarfone vd., 2008).

Belirtilerin tespit edilmesi, organizasyona siber olay meydana gelmeden önlem alabilme fırsatı sunmakla birlikte her saldırının belirtilerle tespit edilmesi mümkün değildir. Zira gerçekleşmeden önce bazı saldırıların bilinen herhangi bir belirtisi olamayabilmekte veya saldırgan belirtileri gizleyebilmektedir (Scarfone vd., 2008).

b.4 Ağ hizmetlerini sunan kişilerle koordinasyonun sağlanması

Siber olayın bertaraf edilmesi amacıyla yürütülen düzeltici faaliyetlerin çoğu, filtre uygulanması, yönlendirme tablolarının güncellenmesi gibi önlemlerin alınmasını zorunlu kıldığı için hizmet alınan internet servis sağlayıcının (İSS) desteğini gerektirebilmektedir. Bunlara ilaveten, olaya ilişkin İSS'nin sistemlerinde de korunması gereken deliller bulunabilmektedir (Northcutt, 2003).

b.5 Siber olayın analizi

Siber olayların tespiti ve analizi zor bir süreçtir. Öncül ve ardıl tüm belirtilerin doğruluğunun kesin olması olayın tespit edilmesini ve analiz edilmesini oldukça kolaylaştırmaktadır. Ancak belirtilerin asılsız ya da yanlış çıkma olasılığı yüksektir. Saldırı tespit sistemlerinin de yanlış pozitif sonuçlar üretebildiği bilinmektedir. Her bir belirtinin doğrulanmaya ihtiyacı vardır. Bu doğrulamanın yapılabilmesi,

kişilerden ve sistemlerden gelen binlerce hatta milyonlarca belirtinin analiz edilerek meydana gelmiş bir olaya ilişkin bilgilere ulaşılması ile mümkün olabilmektedir. Bu durumda siber olaylarla mücadele eden ekiplerin, tespit edildiği ana kadar bir siber olayın meydana gelmekte olduğunu varsaymaları ve buna göre önlemler almaları önerilmektedir (Scarfone vd., 2008).

Siber olaya ilişkin ilk analiz zor bir süreçtir ve bu sürecin kolay ve etkin bir şekilde yapılabilmesi için çeşitli öneriler yapılmaktadır (Scarfone vd., 2008):

- Ağın ve sistemlerin profili ortaya konularak, meydana gelmesi muhtemel siber olayın ağda ve sistemlerde yol açtığı değişiklikler takip edilebilecektir.
- STİM personelinin ağın, sistemin ve uygulamaların normal davranışları ve işleyişi hakkında bilgi sahibi olmaları, ağdaki ve sistemlerdeki sıra dışı durumları fark etmelerini kolaylaştıracaktır.
- Günlük kayıtlarının merkezi sunucularda tutulması ve bir günlük kaydı tutma politikasının olması suretiyle siber saldırıların günlük kaydı tutulmasını devre dışı bırakmalarının önüne geçilecektir.
- Siber olaya müdahale eden personelin kullanabileceği bir bilgi bankasının kurulması ve kullanılması yararlı olacaktır.
- Olaya ilişkin daha fazla bilgiye ihtiyaç duyulması durumunda paket izleme araçları kullanılarak ilave verilerin elde edilmesi sağlanacaktır.
- Deneyimli personel analiz sürecini hızlandıracaktır.
- Daha az deneyimi olan personel için tespit matrisi hazırlanması yararlı olacaktır.
- İhtiyaç halinde başkalarından yardım istenmesi çözümü hızlandıracaktır.

b.6 Olayın önceliklendirilmesi

Siber olayın ele alınması sürecindeki en kritik karar noktalarından biri olayın önceliklendirilmesidir. Kaynakların sınırlı olmasının bir sonucu olarak olayların ilk gelen ilk ele alınır mantığı ile yönetilmemesi gerekmektedir. Bunun yerine siber olay, iki faktör göz önünde bulundurulmak suretiyle önceliklendirilerek ele alınmalıdır (Scarfone vd., 2008):

1. Olaya müdahale eden personelin, olayın sadece mevcut olumsuz teknik etkilerini dikkate almaması, aynı zamanda gelecekte yol açabileceği hasarları da hesaba katması gerekmektedir.
2. Siber olaylara müdahale edilirken kritik kaynakları etkileyen saldırıların önceliklendirilmesi gerekmektedir.

STİM'e ihbar edilen siber olayların, etkilenen sistemlerin önem derecesine göre bir önceliklendirme tablosu esas alınarak önceliklendirilmesi mümkündür (Tablo 1.7).

Tablo 1.7. Siber olayların etki dereceleri

Değer	**Derece**	**Açıklama**
0.00	Yok	Olayın herhangi bir birime veya kritik altyapıya etkisi yok.
0.10	Asgari	Olayın tek bir birim üzerinde ihmal edilebilir bir etkisi var.
0.25	Düşük	Olayın tek birim üzerinde orta derecede bir etkisi var.
0.50	Orta	Olayın tek bir birim üzerinde ciddi etki veya birden fazla birim ya da kritik altyapı üzerinde ihmal edilebilir etkisi var.
0.75	Yüksek	Olayın birden fazla birim veya kritik altyapı üzerinde orta derecede bir etkisi var.
1.00	Kritik	Olayın birden fazla birim veya kritik altyapı üzerinde ciddi bir etkisi var.

Kaynak (Scarfone vd., 2008)

Etki derecelerinin belirlenmesinden sonra olaydan etkilenen sistemlerin kritiklik derecelerinin belirlenmesi de gerekmektedir (Tablo 1.8).

Tablo 1.8 Sistemlerin kritiklik dereceleri

Değer	Derece	Açıklama
0.10	Asgari	Kritik olmayan sistem veya altyapı
0.25	Düşük	Bir tek birime destek veren ancak kritik olmayan sistem(ler)
0.50	Orta	Bir tek birim için kritik olan sistem(ler)
0.75	Yüksek	Birden çok kuruma veya kritik altyapılara destek veren sistem(ler)
1.00	Kritik	Birden çok birim veya kritik altyapılar için kritik olan sistem(ler)

Kaynak (Scarfone vd., 2008)

Siber olayların etkisinin belirlenmesinde Tablo 1.7 ve Tablo 1.8 birlikte kullanılarak bir değerlendirme yapılmaktadır.

b.7 Olayın duyurulması

Vakit geçirilmeden raporlandıklarında siber olayların ele alınması süreci çok daha kolay olabilmektedir. Bu avantajdan faydalanmak için, ilgili ekibin en kısa sürede medyana gelen siber olaydan haberdar edilmesi gerekmektedir (Northcutt, 2003).

Siber olayın analiz edilmesi ve önceliklendirilmesini müteakip organizasyondaki uygun kişilere, bazen de diğer organizasyonlara zamanında yapılan uyarılar, ilgili tarafların bir an önce rollerinin gereğini yerine getirmelerine imkân vermektedir. Günümüzdeki siber tehditlerin ve olayların büyüklüğü ve karmaşıklığı dikkate alındığında siber olaylara işbirliği içerisinde karşı koymanın en etkili yaklaşım olduğunu söylemek mümkündür. Olayın kimlere ne zaman duyurulacağı gibi konuların politikalarda belirlenmiş olması gerekmektedir (Scarfone vd., 2008).

b.8 Olayın belgelendirilmesi

Siber olayın meydana geldiği şüphesinin ardından, olaya ilişkin tüm unsurların gerek fiziki ortamda gerek elektronik ortamda kayıt altına alınmaya başlanması gerekmektedir. Sistemlerdeki aktivitelerin, telefon görüşmelerinin ve dosyalarda meydana gelen değişikliklerin kaydedilmesi sorunun daha etkin ve en az hata ile çözülmesine katkı sağlamaktadır (Scarfone vd., 2008).

Siber olayın tespit edilmesinden sona ermesine kadarki sürecin her adımının belgelendirilmesi ve zaman damgası ile damgalanması, soruna sonradan müdahil olan personelin olay hakkında bilgilenmesini kolaylaştırmaktadır. Bu amaçla belgelendirmenin;

- Olayın mevcut durumunu,
- Olayın bir özetini,
- Söz konusu olaya ilişkin personel tarafından yürütülen tüm faaliyetleri,
- Diğer ilgili tarafların irtibat bilgileri,
- Olayın incelenmesi sürecinde elde edilen delillerin listesini,
- Olaya müdahale eden personelin yorumlarını ve
- Bundan sonra atılacak adımları

içermesi gerekmektedir (Scarfone vd., 2008).

c. Kuşatma, imha etme ve kurtarma aşaması

Siber olayın kapsamını ve büyüklüğünü sınırlamayı amaçlayan kuşatma aşamasında, olay hakkında doğru ve sıcak bilgilerin elde edilebilmesi amacıyla, personelin olay yerinde incelemelerde bulunması söz konusu olabilmektedir. Zira olayın üzerinden bir süre geçmesi durumunda bazı bilgilere ve delillere ulaşılamaması ihtimali bulunmaktadır. Ayrıca kuşatma aşamasında saldırganların sistemlere kötücül kodlar yüklemesinin önüne geçilmesine de dikkat edilmesi gerekmektedir (Northcutt, 2003).

İmha etme aşamasında ise, sistem güvenliğinin tehlikeye düşmesini sonuç veren faktörlerin tamamen ortadan kaldırılması veya azaltılması amaçlanmaktadır. Bir sistemin ele geçirilmesinin sistemin sahibi açısından kötü sonuçları olabilmekte, siber olayı ele alan ekibin sorunu ortadan kaldırmakta başarısız olması yönetimin STİM'in varlığını sorgulamasına yol açabilmektedir (Northcutt, 2003).

Kurtarma aşamasında, siber olaydan etkilenen sistemlerin tamamen çalışır duruma getirilmesi için çeşitli çalışmalar yapılmaktadır.

c.1 Kuşatma stratejisinin belirlenmesi

Bir siber olayın, organizasyonun kaynaklarını tüketecek seviyede yayılmadan kuşatılması büyük önem arz etmektedir. Birçok siber olayla ancak olayı kuşatarak mücadele edilebilmektedir. Dolayısıyla kuşatma çalışmalarını geciktirmeden başlatmak olayın bertaraf edilmesinde son derece önemlidir. Kuşatma sürecindeki en kritik nokta sistemin kapatılması, internet bağlantısının kesilmesi gibi alınacak önlemlere karar verilmesidir. Bir kuşatma stratejisinin olması ve alınacak önlemlerin söz konusu stratejide yer alması karar almayı kolaylaştıracaktır (Scarfone vd., 2008).

Kuşatma stratejileri siber olayın türüne göre farklılık gösterebilmektedir. Büyük türdeki siber olaylar için farklı kuşatma stratejilerinin belirlenmesinde yarar görülmektedir. Kuşatma aşamasında hızlı ve etkin kararların alınabilmesi uygun stratejinin belirlenmesine bağlıdır. Dolayısıyla kriterlerin açık ve net bir şekilde ifade edilmesi gerekmektedir. Söz konusu kriterlerin:

- Siber olayın kaynaklarda yol açması muhtemel hasarlar ve kaynakların çalınması,
- Delillerin korunmasına duyulan ihtiyaç,
- Organizasyon tarafından sunulan hizmetlerin erişilebilirliği,
- Stratejiyi uygulamak için ihtiyaç duyulan zaman ve kaynaklar,
- Stratejinin etkinliği,
- Çözümün süresi

konularını kapsaması gerekmektedir (Scarfone vd., 2008).

Bazı durumlarda siber olayın davranışlarını izlemek ve böylece daha fazla veri elde etmek amacıyla kuşatma faaliyetlerine hemen geçmeden bir süre beklenmesi gerekebilmektedir. Ancak bu durumun sağladığı avantajlar gibi dezavantajları da olabilmektedir (Scarfone vd., 2008). Zira siber suç işleyenler, saldırganların tespit edilmesine yardımcı olan delilleri yok etmede giderek uzmanlaşmaktadırlar. Dolayısıyla şüpheli vakaların gözlendiği sistemlerin tam bir yedeğinin alınması, delillerin saklanması bakımından yararlı olacaktır (Northcutt, 2003).

c.2 Delillerin toplanması ve işlenmesi

Siber olayla ilgili delillerin toplanmasının temel amacı olayın bertaraf edilmesidir. Ancak bu delillerin yasal takibat sürecinde kullanılması da söz konusu olabilmektedir. Bu durumda delillerin nasıl korunması gerektiğinin açık bir şekilde belirlenmesi ve belgelendirilmesi gerekmektedir. Bunun yanı sıra delil toplama süreçlerinin mevzuata uygun olmasına dikkat edilmelidir. Zira delillerin mahkeme tarafından kabul görmesi yasalara uygun toplanmasına bağlıdır (Scarfone vd., 2008).

Tüm deliller için:

- Bilgiyi tanımlayan parametreleri (bir bilgisayarın internet protokolü (Internet Protocol - IP) adresi, lokasyonu, seri numarası vb.),
- Delili toplayan veya kullanan kişinin adını, unvanını ve telefon numarasını,
- Delilin kullanıldığı zamanı, tarihi ve
- Delilin saklandığı yeri

kapsayan günlük kayıtlarının tutulması, delillerin güvenliğinin ve gizliliğinin sağlanması için bir zorunluluk olarak görülmektedir (Scarfone vd., 2008).

c.3 Bilgisayarlar için adli bilişim çalışmaları

Saldırgan tarafından ele geçirilen sistemlere ilişkin yapılması gerekenlere karar verilmesi oldukça zor bir süreçtir. Sistemin kapatılmasına, internet bağlantısının

kesilmesine ya da çalışmaya devam etmesine karar verilirken kapsamlı bir değerlendirme yapılması gerekmektedir (Northcutt, 2003).

Olaydan etkilenen sistemlerdeki dosyalar kopyalanmadan önce, herhangi bir dosyaya kayıtlı olmayan o anki ağ bağlantıları, koşan işlemler, açık oturumlar, açık dosyalar ve hafızanın içeriği gibi kalıcı olmayan bilgilerin yakalanması önerilmektedir. Zira bu yolla elde edilecek bilgiler saldırganın kimliğine veya saldırıda kullanılan yönteme ilişkin ipuçları içerebilmektedir (Scarfone vd., 2008).

Ele geçirilen sistemlerde yapılacak herhangi bir işlem sistemin o anki durumunu değiştirecektir. Bu durumda hem saldırganın siber olayla mücadele edildiğinin farkına varması (Scarfone vd., 2008) hem de sistemdeki delillerin zarar görmesi söz konusu olabilmektedir.

c.4 Mobil cihazlar için adli bilişim çalışmaları

Georgia Tech Üniversitesi'nden Yardımcı Doçent Patrick Traynor;

> Dünyadaki cep telefonu kullanıcılarının sayısı proaktif mobil güvenlik önlemleri alınmasının bir ihtiyaç olduğunu göstermektedir. Günde 1.5 milyar kişinin internet kullanmasına karşın, 4.5 milyardan fazla kişi cep telefonu kullanmakta ve bu durum siber suçlular için cazip bir hedef oluşturmaktadır. Önümüzdeki 5-10 yılda bu rakamlar iki veya üç katına çıkacaktır.

yorumunu yapmaktadır (GTISC, 2011).

Yine M.A.D. Partners şirketinin kurucusu olan Rober Smith, herhangi bir kuruluşu tehdit eden tek büyük şeyin mobil cihazlar olduğunu söylemektedir. Smith ayrıca, cep telefonu uygulama mağazalarının, bugüne kadar insan tarafından icat edilen en büyük kötücül yazılım dağıtma sistemi olduğunu ifade etmektedir (GTISC, 2011).

Kullanımı her geçen gün yaygınlaşan ve internete bağlı olan mobil cihazların suçluya seyyar olma ve mobil bağlantı fırsatı vermesinin, siber suçlarla mücadelede artan miktarda zorlukları beraberinde getireceği yorumları yapılmaktadır (Demir ve Küçükuysal, 2011).

Yukarıdaki görüşlerden, kullanımı bilgisayarlardan daha yaygın olan ve kuruluşlar için önemli bir güvenlik noktası haline gelen mobil cihazlar için güvenlik önlemlerinin alınması gerektiği anlaşılmaktadır.

GTISC bünyesinde mobil güvenlik konusunda çeşitli araştırmalar yapılmaktadır. Bunlardan biri, cep telefonuna gelen çağrının kaynağının ve takip ettiği yolun tespit edilmesine yönelik bir araştırmadır. Çalışmanın sonunda kullanıcıların, çağrıların gerçekten nereden geldiğini ve takip ettiği yolu tespit edebilmeleri amaçlanmaktadır (GTISC, 2011).

Yine GTISC bünyesindeki diğer bir araştırma ise, mobil telefonlardaki kötücül yazılım problemlerinin aşılmasına ilişkindir. *"Uzaktan Onarma"* adlı proje ile kötücül yazılımdan etkilenen mobil cihazın, tamir için mağazaya gitmesi yerine, kullanıcıların telefon firmasından veya üçüncü bir taraftan uzaktan yardım almasına imkân verileceği ifade edilmektedir. Mobil saldırılar arttıkça bu tür çözümlere daha çok ihtiyaç duyulacağı öngörülmektedir (GTISC, 2011).

Organizasyonlarda mobil cihazların oldukça fazla kullanıldığı, siber olayların mobil cihazları da kapsayacak şekilde arttığı dikkate alındığında, adli bilişim çalışmalarının mobil cihazlar için de yapılması gerektiği görülmektedir. Yukarıda adı geçen projelerin ve çalışmaların, mobil cihazlara yönelik adli bilişim çalışmalarında önemli katkılar sağlayacağını söylemek mümkündür.

c.5 Saldırganın tespit edilmesi

Siber olaylarla mücadelede saldırganın tespit edilmesi doğal olarak istenen bir sonuçtur. Siber saldırının hedefi olan organizasyonun, saldırganın soruşturulmasını istemesi durumunda kimlik tespiti önem kazanmaktadır. Kimlik tespitinin yapılabilmesi için siber olayla mücadele eden ekibin kuşatma, imha etme ve kurtarma aşamasına yoğunlaşması önerilmektedir. Kimlik tespiti zaman alan bazen de sonuç alınamayan bir süreç olabilmektedir. Saldırganın tespit edilmesinde çeşitli yöntemler kullanılmaktadır (Scarfone vd., 2008):

- Saldırganın IP adresinin doğrulanması,
- Saldırganın sisteminin taranması,
- Arama motorlarından saldırganın araştırılması,
- Olay veritabanlarının kullanılması,
- Saldırgana ait muhtemel iletişim kanallarının izlenmesi.

Ne olduğu bilinmezse sistemlerin ele geçirilmesine yol açan güvenlik probleminin çözümü de mümkün olmamaktadır. Olanların anlaşılması amacıyla saldırının izole edilerek nasıl çalıştığının belirlenmesi, siber olayın sebeplerinin ve belirtilerinin anlaşılması bakımından önem arz etmektedir (Northcutt, 2003). Zira siber olayın kuşatılmasının ardından, olayın bileşenlerini ortadan kaldırmak amacıyla kötücül kodların silinmesi veya ihlale yol açan kullanıcı hesaplarının devre dışı bırakılması gibi imha faaliyetlerinin başarılı olması, olay hakkında sahip olunan bilgilere bağlıdır. Bir anlamda siber olayın kalıntılarının temizlenmesi aşaması olarak da adlandırılabilecek imha aşamasında (Scarfone vd., 2008), olayın meydana gelmesine yol açan sebeplerin ortadan kaldırılması için de çalışmalar yapılmasının aynı olayın gelecekte tekrar yaşanmasının engellenmesine katkı sağlayacağı düşünülmektedir. Herhangi bir siber saldırıya maruz kalmamış en güncel sistem yedeklerinin yüklenmesini, imha sürecinin son aşaması olarak değerlendirmek mümkündür (Northcutt, 2003).

İmha sürecinin hemen ardından kurtarma süreci olarak adlandırılan aşamada, sistemlerin yeniden hizmet verebilir duruma getirilmesi, problemin tamamen ortadan kaldırıldığından emin olunması amacıyla sistemlerin doğrulanması (Northcutt, 2003) çalışmaları yürütülmektedir. Kurtarma aşamasında sistem yöneticileri tarafından sistemlerin normal işleyişine kavuşturulması ve benzer siber olayların tekrar meydana gelmesi ihtimaline karşılık sistemlerin sağlamlaştırılması işlemleri gerçekleştirilmektedir. Zira genelde bir sisteme yapılan saldırının başarılı olması durumunda aynı sisteme veya ilgili organizasyondaki başka sistemlere benzer saldırılar yapılmaktadır (Scarfone vd., 2008).

d. Olay sonrası faaliyetler

Olay sonrası faaliyetlerin amacı, meydana gelen saldırılardan dersler çıkarmaktır. Yaşanan problemler, gelecekte daha iyi çalışmaların yapılması için kişileri araştırmaya yöneltmektedir. Stres seviyesinin yüksek ilişkilerin gergin olduğu siber olayın yaşanması sürecinin ardından, personelin yaşanan durumu unutmasının önüne geçilmesi amacıyla olaydan sonra yapılan çalışmaların siber olaylarla mücadele kapasitesini arttırdığı görülmüştür (Northcutt, 2003).

d.1 Çıkarılan dersler

Siber olaylara müdahale ekibinin, yeni tehditler, gelişen teknolojiler ve yaşanan olaylardan edinilen deneyimlere sahip olması ve bu deneyimleri müdahale süreçlerinde kullanması beklenmektedir. Siber olaylardan sonra ya da periyodik olarak ilgili tüm taraflarla, olaylardan alınan derslere ilişkin bir toplantının yapılmasının, alınan güvenlik önlemlerinin ve siber olaylara müdahale süreçlerinin geliştirilmesinde son derece yararlı olduğu vurgulanmaktadır. Söz konusu toplantılarla (Scarfone vd., 2008):

- Tam olarak ne oldu ve ne zaman oldu?
- Personel ve yönetim siber olayı ne kadar başarılı yönetebildi? Dokümante edilen prosedürler takip edildi mi ve bu prosedürler yeterli miydi?
- Olaya müdahale sürecinde hangi bilgilere ihtiyaç duyuldu?
- Kurtarma sürecine olumsuz etkisi olan ya da süreci önleyen bir adım atıldı mı?
- Benzer bir siber olayın yeniden olması durumunda personelin ve yönetimin farklı olarak ne yapması gerekir?
- Hangi düzeltici faaliyetler benzer olayların gelecekte de yaşanmasını önler?
- Gelecekte siber olayları tespit etmek, analiz etmek ve bunlarla mücadele etmek için ihtiyaç duyulan ilave araçlar ya da kaynaklar nelerdir?

gibi sorulara cevap aranmaktadır.

Olay sonrası yürütülmesinde yarar görülen faaliyetler arasında, meydana gelen her siber olaya ilişkin bir raporun hazırlanması yer almaktadır. Bu rapor gelecekte benzer

olayların olması durumunda olaya müdahale edilirken kullanılabilmektedir. Siber olayların kronolojik bir şekilde arşivlenmesi hem yasal çalışmalara hem de meydana gelen hasarların tespitine yardımcı olmaktadır (Scarfone vd., 2008).

d.2 Elde edilen olay verilerinin kullanılması

Yaşanan olaylardan edinilen tecrübelerin çeşitli objektif ve sübjektif sonuçlara dönüştürülmesi, yeteneklerin daha da geliştirilmesine katkı sağlamaktadır. Özellikle bir olayla mücadeleye ayrılan süre ve olayın getirdiği maliyet gibi veriler, olaya müdahale ekibine ilave finansman sağlanmasına karar verilmesinde kullanılabilmektedir. Olay verilerinin olaylara müdahale ekibinin başarısının ölçülmesinde de kullanılması mümkündür (Scarfone vd., 2008).

Veri toplama işleminde, uygulanabilirliği olan ve politika belirlemede katkısı olabilecek verilerin toplanmasında yarar görülmektedir. Bir yılda maruz kalınan yetkisiz erişim sayısından ziyade, siber tehditlerin kuruluşun iş süreçlerini nasıl etkilediği verisi daha değerli görülmektedir. Dolayısıyla, iş süreçlerinin güvenliğinin arttırılarak iyileştirilmesine ve yatırımlarına değer katacak verileri aşağıda sıralanan hususların dikkate alınarak toplanması hedeflenmelidir:

Müdahale edilen olay sayısı: Müdahale ekibinin çalışma performansının değerlendirilmesinde yararlı olabilmektedir.

Olay başına süre: Her siber olayın bertaraf edilmesi için harcanan sürenin:

- Olay için harcanan toplam işgücü,
- Olayın başlamasından çözülmesine kadar geçen süre,
- Olaya müdahale aşamalarının her birinde geçen süre,
- Olaya ilişkin ilk rapora müdahale ekibinin cevap verme süresi,
- Olay hakkında yönetime veya ilgili taraflara bilgi verilmesi için geçen süre

şeklinde farklı biçimlerde ölçülmesi mümkündür.

Her olayın tarafsız değerlendirilmesi: Bir siber olaya verilen yanıtın ne kadar etkin olduğunun tarafsız bir bakış açısıyla analiz edilmesi, olaya müdahale sürecinde atılan doğru ve yanlış adımların görülmesini kolaylaştırmaktadır.

Her olayın öznel değerlendirilmesi: Ekipte yer alan personelin kendi bakış açısıyla olayları değerlendirmesi, farklı çözüm yaklaşımlarının ortaya çıkmasını sağlamaktadır.

d.3 Delillerin saklanması

Siber saldırganın yargılanması, veri saklama politikası ve getireceği maliyetler dikkate alınarak delillerin ne kadar süre saklanacağına karar verilmesi gerekmektedir (Scarfone vd., 2008).

1.3.3.2. Olaya müdahale kontrol listesi

Siber olaylara müdahalede hızlı ve etkin adımlar atmanın olayın önlenmesine ve oluşabilecek muhtemel hasarların asgariye indirilmesine çok önemli katkıları olmaktadır. Hızlı ve etkin adımların atılması ise ne yapılacağının önceden bilinmesine bağlıdır. Siber olaylara ilk müdahale edilirken yapılması gereken önemli işlemleri gösterir bir başlangıç kontrol listesinin takip edilmesi önerilmektedir (Tablo 1.9).

Tablo 1.9. Siber olaya müdahalede başlangıç kontrol listesi

No	Eylem	Tamamlandı
	Tespit ve analiz aşaması	
1.	Bir olayın meydana gelip gelmediğini tespit edin.	
1.1	Öncül ve ardıl belirtileri analiz edin.	
1.2	Bilgiler arasında bağlantı kurmaya çalışın	
1.3	Arama motorlarından veya bilgi bankalarından araştırma yapın.	

1.4	Siber olayın meydana geldiğine inanıyorsanız araştırma ve delil toplama işlemlerini dokümante edin.	
2.	Tespit ve analiz aşamasında verilen olay kategorileri tablosuna göre olayı sınıflandırın (DoS, kötücül kod, yetkisiz erişim gibi).	
3.	Uygun olaya ait kontrol listesini takip ediniz. Olay herhangi bir kategoriye girmiyorsa genel kontrol listesini takip ediniz.	

Kaynak: (Scarfone vd., 2008)

Müdahale edilen siber olay, kategori tablosunda belirtilen olay türlerinden biri ile eşleştirilebiliyorsa ilgili olaya ilişkin önceden hazırlanmış kontrol listesinin takip edilmesi, aksi halde genel kontrol listesinin takip edilmesi gerekmektedir (Tablo 1.10).

Tablo 1.10. Sınıflandırılmamış siber olaylara müdahalede genel kontrol listesi

Eylem	Açıklama	Tamamlandı
Tespit ve analiz aşaması	1. Siber olaylara iş süreçlerine olabilecek etkilerine göre müdahale önceliği veriniz.	
	1.1. Etkilenen kaynakları tespit, etkilenmesi muhtemel kaynakları tahmin ediniz.	
	1.2. Olayın mevcut ve muhtemel teknik etkilerinin neler olabileceğini değerlendirin.	
	1.3. Teknik etkilere ve etkilenen kaynaklara göre önceliklendirme matrisinde uygun hücreleri bulunuz.	
	2. Organizasyon içindeki uygun personele ve diğer organizasyonlara olayı rapor edin.	
Kuşatma, imha etme ve kurtarma aşaması	3. Delilleri edinin, muhafaza edin ve delillerin güvenliğini sağlayın.	
	4. Siber olayı kuşatma altına alın.	
	5. Siber olayı imha edin.	
	5.1. İstismar edilen tüm açıklıkları tespit edin ve önlem almaya çalışarak sayılarını azaltın.	
	5.2. Kötücül kodları, uygun olmayan materyalleri ve bileşenleri kısaca siber olayın kalıntılarını sistemlerden çıkarın.	
	6. Sistemleri kurtarma işlemlerini gerçekleştirin.	

	6.1. Etkilenen sistemleri işlevsel duruma hazır hale getirin.	
	6.2. Etkilenen sistemlerin normal çalıştığını doğrulayın.	
	6.3. Geleceğe ilişkin faaliyetlere bakmak için gerekirse sistemlere ilave izleme adımları uygulayın.	
Olay sonrası faaliyetler	7. Gelecekte kullanılmak üzere bir takip raporu oluşturma.	
	8. Olaydan edinilen derslerin değerlendirileceği bir toplantı yapın.	

Kaynak: (Scarfone vd., 2008)

1.3.4. STİM İşbirliği Yaklaşımları

Ülkeler arasında bağlantı kurulmasına olanak sağlayan internet ve BİT'ler, ülkelerin kendilerini hedef alan siber tehditlere sınırlarını kapatma imkânını ortadan kaldırmaktadır. Bu tür sorunları çözmek için ulusal veya bölgesel düzeyde yapılan girişimler önemli olmakla birlikte yeterli görülmemektedir. İnternet gibi küresel ve geniş kapsamlı bir konu olarak değerlendirilen siber güvenlik alanındaki çözümlerin de sınır aşan bir şekilde uyum içinde üretilmesi gerekmektedir. Bu durum, sadece devlet düzeyinde değil, sektör ve sivil toplum kuruluşları düzeyinde uluslararası işbirliğini zorunlu kılmaktadır (ITU, 2007a).

Her ülkenin hemen her gün diğer bir ülkenin yardımına ihtiyaç duyduğu bir konu olan siber suçlar, suçun önlenmesi ve soruşturulması bağlamında işbirliğine en çok ihtiyaç duyulan bir alan olarak değerlendirilmektedir. Zira internet ortamının bütün ülkeleri birbirine aynı yakınlıkta komşular haline getirdiği bir ortamda siber âlemde, büyük aktörlere sahip olan ve en çok suçluyu barındıran ülkelerle işbirliğine gidilmesi önerilmektedir (Demir ve Küçükuysal, 2011).

Ülkelerin, iş dünyasının ve kar amacı olmayan kuruluşların siber tehditlere ve bu tehditlere karşı koyma uygulamalarına ilişkin bilgi paylaşımında bulunmaları siber tehditlerle mücadelenin anahtar parametreleri arasında sayılmaktadır. Bilgi altyapılarının korunması ve siber suçlarla mücadele edilmesi için, ülkelerin siber tehditleri değerlendirecekleri, önleyecekleri, bu tehditlere karşı koyacakları ve siber

olaylardan sonra sistemleri geri kurtaracakları yapılara ve sistemlere bir diğer deyişle STİM'e sahip olmaları gerekmektedir (ITU, 2007b).

Bilgi paylaşımı, bazı ülkelerde STİM'ler aracılığıyla yapılmasına karşın bazı ülkelerde özel sektör tarafından finanse edilen bilgi paylaşımı ajansları aracılığı ile yapılmaktadır. Örneğin İngiltere'de uyarı, tavsiye ve raporlama noktalarının (Warning, Advice and Reporting Points - WARPs) kurulması konusunda çalışmalar yürütülmektedir (ITU, 2007b).

Bilgi paylaşımı ve işbirliği her siber güvenlik organizasyonunun öncelikli olarak gündeminde olması gereken bir konudur. Sadece ulusal gruplarla değil uluslararası kamu ve özel ortaklarla da işbirliği kurulması siber olayların sınır aşan doğasının bir gereğidir.

Edison Electric Institute yöneticilerinden David Batz'ın,

> Düşmanlarımız birbirleriyle bilgi paylaşma konusunda çok yetenekliler. Tehditlere karşı mücadele eden bizlerin, daha etkin bilgi paylaşımında bulunmak ve güvenlik konusunda daha fazla ilerleme kaydetmek için yapısal iletişimi geliştirme konusunda neler yapılması gerektiğini öğrenmek zorundayız.

görüşünden, siber tehditlerle mücadelede başarılı olmak için olaylara müdahalede özellikle de bilgi paylaşımında en az siber saldırganlar kadar yetenekli olunması gerektiği anlaşılmaktadır (GTISC, 2011).

Özellikle bilgi paylaşımında ve siber tehditlerle mücadelede başarılı olunmasında birçok alanda olduğu gibi gerçekleştirilecek işbirliği ve bilgi paylaşımının önemi büyüktür. İşbirliğinde ortak bir dilin kullanılması ve ortak bir bakış açısının geliştirilmesi işbirliğinin ve paylaşımın etkinliğini önemli ölçüde arttırmaktadır.

1.3.4.1. İşbirliğinin yasal dayanağı

STİM'ler arasında gerçekleştirilen işbirliği çalışmalarının faklı yasal dayanakları olabilmektedir. Birçok durumda özellikle de ikili işbirlikleri gayrı resmi olarak

gerçekleşebilmektedir. İşbirliğinin resmileştirilmesi ihtiyacının duyulması durumunda farklı yollar söz konusu olabilmektedir. İşbirliğinin resmileştirilmesinin gerekçeleri arasında mali nedenler, yasal gereksinimlerin belirlenmesi veya hassas verilerin paylaşılması sayılmaktadır (ENISA, 2006b).

STİM'ler veya STİM toplulukları arasında kurulan işbirliklerinin resmileştirilmesinde gizlilik anlaşması, mutabakat zaptı, sözleşme veya iş tanımı gibi belgeler kullanılabilmektedir.

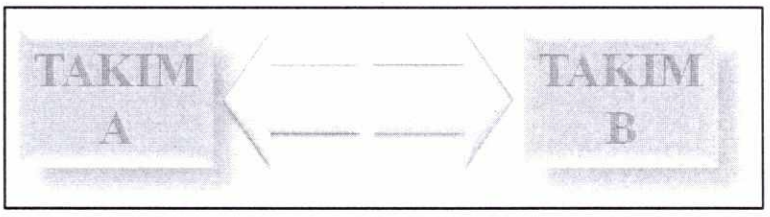
1.3.4.2. İşbirliği modelleri

Çok çeşitli işbirliği modelleri bulunmakla birlikte STİM dünyasında en çok karşılaşılan bazı modeller vardır. Bu modellerin sadece STİM'ler tarafından kullanılmadığını belirtmekte yarar vardır (ENISA, 2006b).

a. İkili işbirliği (takım-takım)

Sadece iki STİM arasında bir işbirliği söz konusu olduğu ikili işbirliği modeli (Şekil 1.11), takımlar ve takım çalışanları arasındaki güvene dayanmaktadır (ENISA, 2006b).

Şekil 1.11. İkili işbirliği modeli



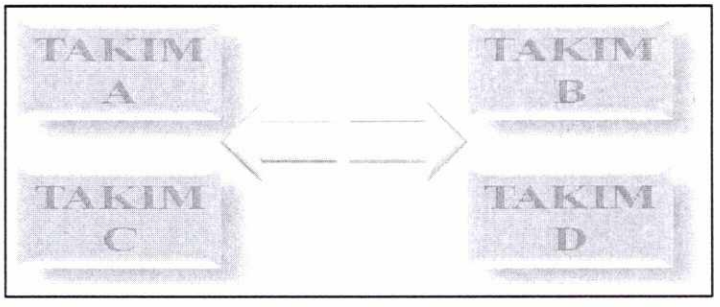
İkili işbirliği modelinin genellikle geleceğe ilişkin ortak hedefleri ve benzer misyonları olan STİM'ler arasında kullanıldığı ifade edilmektedir. Takımlar işbirliği ilişkilerini yazılı bir anlaşma ile resmileştirmeyi tercih etmektedirler (ENISA, 2006b).

İkili işbirliği modelinin oldukça etkili bir model olduğu görülmektedir. Zira bu modelde takımların ortaklaşa belirledikleri hedeflere odaklanmaları söz konusudur. Koordine edilmesi gereken işlerin az olmasından dolayı ikili işbirliği modelinin yönetilmesinin kolay olduğunu söylemek mümkündür. Ayrıca bu işbirliği modelinin doğası gereği genel etkisi sınırlıdır ve sonuçlarından çoğunlukla sadece işbirliği kuran takımlar yararlanmaktadır. Dolayısıyla geniş bir yelpazenin yararlanacağı yeni bir standardın hazırlanması söz konusu ise daha fazla tarafın görüşlerinin alınabilmesi için farklı bir işbirliği modelinin seçilmesinde yarar görülmektedir (ENISA, 2006b).

b. Ortaklık

Ortaklık işbirliği modeli (Şekil 1.12) ortak ilgi alanları ve hedefleri olan birçok takım arasında kurulan bir işbirliği modelidir. Bu tür işbirliğinin çerçevesinin ortak bir coğrafi bölge, ortak hizmetler, benzer müşteriler ve sektörleri dikkate alınarak belirlenmesi önerilmektedir (ENISA, 2006b).

Şekil 1.12. Ortaklık işbirliği modeli



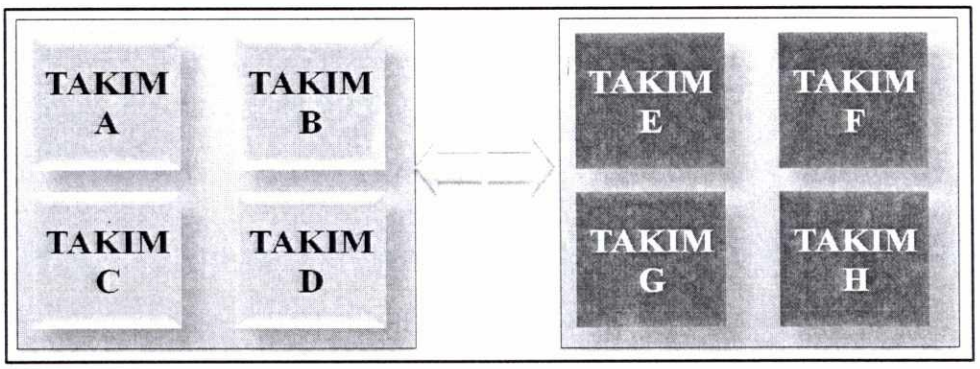
Ortaklık işbirliği modellerinde forum, görev gücü, grup, koalisyon veya ittifak gibi farklı isimlerin kullanıldığı görülmektedir. Ortaklık işbirliğine, Olaylara Müdahale ve Güvenlik Ekipleri Forumu (Forum of Incident Response and Security Teams - FIRST), Trans-Avrupa Araştırma ve Eğitim Ağı Birliği (Trans-European Research and Education Networking Association - TERENA) Görev Gücü STİM (Task Force CSIRT - TF-CSIRT) ve Asya-Pasifik STİM (Asia-Pasific CERT - APCERT) örnek olarak verilebilir. İkili işbirliklerinin etkin bir şekilde gelişmesi için çeşitli

organizasyonel araçlar, yönetim kurulu, başkan ve sekreterya gibi resmi organlara gereksinim duyulmaktadır (ENISA, 2006b).

c. Ortaklıklar arası işbirliği

Ortaklıklar arası işbirliği iki veya daha fazla sayıdaki ortaklık arasında kurulan işbirliği modelidir (Şekil 1.13). Bu modelde de ortaklıkların benzer hedeflerinin ve çıkarlarının ön planda olduğunu söylemek mümkündür (ENISA, 2006b).

Şekil 1.13. Ortaklıklar arası işbirliği modeli



Ortaklıklar arası işbirliğinde daha çok taraflar arasında tecrübeler paylaşılmakta ve işbirliğinin ortak hedefleri ve kuralları belirlenmektedir. TERENA TF-CSIRT ve APCERT ortaklık işbirliğine verilebilecek örnekler arasında yer almaktadır (ENISA, 2006b).

1.3.4.3. İşbirliğinde güven

İşbirliğinin en önemli parametrelerinden biri tarafların birbirlerine duydukları güvendir. STİM gibi hassas verilere sahip olan organizasyonlar ve bu verilerin paylaşılması söz konusu olduğunda taraflar arasındaki güven daha da önem kazanmaktadır. Dolayısıyla STİM'ler arasında işbirliğinin sorunsuz olarak gerçekleşebilmesi için öncelikle taraflar arasında güvenin tesis edilmesi gerekmektedir.

Birçok durumda operasyonel veriler özel veya hassas olarak değerlendirilmektedir. Ancak diğer taraftan arındırılarak özel veya hassas olmaktan çıkarılan verilerin

paylaşılması, verileri alan tarafın ilave bazı çalışmalar yürütmesini gerektirebilmekte dolayısıyla iş yükünü arttırmaktadır. Gerekli durumlarda verilerin arındırılmadan da paylaşılmasının sağlanması gerekmektedir. Dolayısıyla bilgi paylaşımının etkin olabilmesi için taraflar arasında güven oluşturacak çeşitli yöntemlerin uygulanması gerekmektedir (ENISA, 2006b).

a. İkili ve çok taraflı anlaşmalar

İşbirliğinde güvenin tesis edilmesinde kullanılan en basit yöntem taraflar arasındaki işbirliğinin ve veri paylaşımının kapsamını belirleyen bir yasal dokümanın imzalanmasıdır. Burada imzalanan dokümanın tüm tarafları hukuken bağlamasına dikkat edilmesi gerekmektedir. Pratikte bir mutabakat zaptının veya sözleşmenin ikiden fazla tarafı ilgilendirmediği ifade edilmektedir (ENISA, 2006b).

Bir diğer yöntem yasal herhangi bir bağlayıcılığı olmayan davranış kuralları dokümanı oluşturulmasıdır. Bir davranış kuralları dokümanı genellikle belirli bir davranışa ve tarafların kararlarına ilişkin çeşitli kuralları ve ilkeleri içerir. Hukuki bağlayıcılığı olmamasına rağmen davranış kuralları dokümanının imzalanması etik kurallar çerçevesinde hareket edileceğine gösteren bir emare olarak görülmektedir. Avrupa hükümetler işbirliği gibi kapalı topluluklarda işbirliğinin bir üyesi olmak için davranış kuralları dokümanının imzalanması bir zorunluluk olabilmektedir. Bu durumda davranış kurallarının ihlal edilmesi ilgili katılımcının üyelikten atılmasına sebep olabilmektedir (ENISA, 2006b).

b. Sponsorluk

Güvenin tesis edilmesinin bir diğer yolu sponsorluktur. STİM dünyasında bu modelin FIRST tarafından geliştirildiği ifade edilmektedir. Sponsorluk modeli, güven seviyesini açıkça beyan eden bir takımla yakından ilişki kurulmasına dayanmaktadır. Bu şekilde kendisine güvenilen takım üye olmak isteyen yeni takıma sponsor olmaktadır. Üyelik sürecinde sağlanması gereken çeşitli gereksinimler konusunda yeni takıma rehberlik yapmaktadır. Bu süreçte topluluğun diğer üyeleri yeni takımın işbirliği topluluğuna değer katacağı ve kendilerine yarar sağlayacağı

konusunda kendisine güvenilen ve sponsorluk yapan takıma güvenmektedirler (ENISA, 2006b).

FIRST örneğinde sponsora yüklenen en önemli konular arasında:

- Yeni üyeyi katılacağı organizasyon hakkında bilgilendirmek,
- İşbirliği topluluğuna başvuran takımın çalışma ortamı hakkında daha fazla bilgi almak amacıyla yerinde incelemelerde bulunmak,
- Yeni takımı topluluğa tanıtmak ve takımın yaşadığı ilk sorunlarda ilk temas noktası olarak destek vermek
- Başvuru işlemi sürecinde topluluk nezdinde yeni takımı temsil etmek

yer almaktadır (ENISA, 2006b).

c. Açık topluluklar

Tartışılan konulara ilgi duyanların istemeleri durumunda katılabildikleri açık gruplar ve topluluklar bulunmaktadır. Buna, çok yaygın olarak kullanılan ve herkesin katılımına açık olan güvenlik posta listeleri örnek gösterilmektedir.

Açık topluluklarda güvenin tesis edilmesi çok kolay olmamaktadır. Zira bu tür topluluklarda bir kişinin yüksek bir güven seviyesi ile başlaması ve istismar edilene kadar da bu seviyeyi koruması şeklinde bir güven yaklaşımından bahsedilmektedir. Açık topluluk modelinin genellikle özel ilgi grupları ve çalışma grupları tarafından kullanıldığı ifade edilmektedir. Her ne kadar bu modelde katılım ve iletişim teşvik ediliyor olsa da yasalar ihlal edilmeden hassas verilerin katılımcılar arasında paylaşılması mümkün olamamaktadır. Modelin 30-40 gibi daha küçük sayıda üyesi olan topluluklarda sorunsuz olduğunu söylemek mümkündür. Ancak kişi sayısı arttıkça küçük alt gruplara bölünme de söz konusu olabilmektedir.

d. Akreditasyon

İhtiyaç duyulması halinde bir topluluğun üyeleri için bir güven seviyesi kurmak için harici güvenilir üçüncü tarafın yaptığı bir akreditasyon sürecini işletebilmektedir.

Güven seviyesi yüksek alt gruplara izin veren ve çok fazla üyesi olan topluluklar için akreditasyon modelinin faydalı olabileceğini söylemek mümkündür. Akreditasyon modeline TERENA TF-CSIRT ve Trusted Introducer tarafından akredite edilen takımlar örnek olarak verilmektedir (ENISA, 2006b).

1.3.4.4. İşbirliği çeşitleri

Kurulan işbirliklerine bakıldığında aynı ülke sınırları içindeki, aynı bölgedeki veya farklı ülke hatta kıtalardaki STİM'ler arasında çeşitli işbirliklerinin kurulduğu görülmektedir. Bu durumun siber olayların sınır aşan yapısından kaynaklandığını bir kez daha hatırlatmakta yarar görülmektedir. Avrupa çapındaki STİM işbirliğine TF-CSIRT, küresel çaptaki STİM işbirliğine ise FIRST örnek verilmektedir.

Sadece bu bölümde anlatılan işbirliği çeşitleri bulunmamakta, bu çeşitler en belirgin örnekler olarak sayılmaktadır.

a. Ulusal işbirliği

Aynı ülke sınırları içindeki STİM'lerin bir araya gelerek kurdukları bir işbirliği çeşididir. Ulusal işbirliğinin ardındaki ana nedenler olarak, aynı milliyetten olma, aynı dili konuşma, siyasi, ekonomik ve teknik konular hakkındaki ortak bilgiler sayılmaktadır. Ülkede tanınan ulusal bir STİM bulunmuyor ise ulusal işbirliği girişiminin söz konusu ülke için ulusal irtibat noktası olarak faaliyet göstermesi söz konusu olabilmektedir. Ulusal işbirliği girişimleri genellikle devletleri veya bankacılık gibi hassas sektörleri de kapsayan çeşitli sektörlerden takımları bir araya getirmektedirler. Grubun farklı ilgi alanlarının karışımından oluşmasından dolayı mutabakat zaptı gibi bir taahhüt bildirimine ve dış dünyaya sunulan bir misyon bildirisine ihtiyaç duyulmaktadır (ENISA, 2006b).

Ulusal işbirliği çeşitlerine:

- Avusturya ulusal işbirliği (CIRCA.AT)
- İngiliz ulusal işbirliği (UKCERTS)
- Hollanda ulusal işbirliği (o-IRT-o)

- Almanya ulusal işbirliği (CERT-Verbund)

örneklerini vermek mümkündür (ENISA, 2006b).

b. Bölgesel işbirliği

STİM işbirliklerinin en çok bölgesel bağlamda başarılı olduğu ifade edilmektedir. Buna gerekçe olarak da daha fazla toplantı yapmayı teşvik eden kısa seyahat süreleri ve daha düşük maliyetli toplantılar gösterilmektedir. Bir diğer önemli etken olarak da işbirliğine katılan takımların kültürel benzerliklerinin sosyal paylaşımı kolaylaştırması sayılmaktadır. En uzun soluklu ve en olgun bölgesel işbirliklerinin Avrupa'da geliştirildiği, ancak 2003 yılında APCERT'in kurulmasından sonra Asya-Pasifik bölgesinde önemli ilerlemeler kaydedildiği ifade edilmektedir (ENISA, 2006b).

Avrupa'daki çalışmalara bakıldığında, Avrupa sınırları dâhilindeki STİM'ler ile yapılan çeşitli toplantılarda bir koordinasyon merkezine ihtiyaç duyulduğu sonucuna varılmıştır. Bunun üzerine 1995 yılında TERENA tarafından kurulan görev gücü ile mevcut durumun analiz edilmesi ve bir koordinasyon modelinin oluşturulması çalışmaları yürütülmüştür. Görev gücünün çalışmaları sonucunda ortaya çıkan öneriler doğrultusunda Avrupa İçin Güvenlik Olaylarına Müdahale Koordinasyonu (Security Incident Response Coordination for Europe - SIRCE) kurulmuş ve söz konusu merkez 1997 yılında Avrupa STİM (European CERT, EuroCERT) adı altında çok iddialı hedeflerle çalışmaya başlamıştır. EureCERT'in kendisinin bir STİM olması hedeflenmemiştir. Siber olaylara gerçek müdahalelerin katılımcı STİM'ler tarafından yapılması düşünülmüştür.

Asya'daki işbirliklerine bakıldığında ise, Japonya'nın U-STİM'i olan JPCERT/CC, 2002 yılında Japonya'da ilki düzenlenen Asya-Pasifik Güvenlik Olaylarına Müdahale Koordinasyonu (Asia-Pacific Security Incident Response Coordination - APSIRC) toplantısına katılmaları için Asya-Pasifik bölgesinin önde gelen ekonomilerinin STİM'lerini davet ettiği görülmektedir. Toplantıda bölgesel STİM'ler ile işbirliğinin geliştirilmesi tartışılmıştır (ENISA, 2006b).

APSIRC toplantısının sonucunda sınır ötesi bölgesel işbirliğinin hayata geçirilmesi için APCERT birliği kurulması kararı alınmıştır. Sonrasında APCERT'in kurulmasına onay veren 12 ülkeden 15 STİM'in imzalayacağı bir anlaşmanın oluşturulması çalışmaları başlatılmıştır.

APCERT anlaşması APSIRC toplantısının tüm katılımcıları tarafından Şubat 2003'te kabul edilmiş ve yönetim kurulu, başkan ve sekreterya için seçimler yapılmıştır.

APCERT'in hedefleri arasında:

- Asya-Pasifik bölgesinde güvenilir bir bilgisayar güvenlik uzmanları ağı kurmak böylece bölgenin farkındalığını ve bilgisayar güvenlik olaylarına ilişkin yetkinliği:
    - Asya-Pasifik bölgesinin bilgi güvenliği konusunda bölgesel ve uluslararası işbirliğini geliştirerek,
    - Büyük ölçekli veya bölgesel ağ güvenlik olayları ile mücadele etmek için ortak tedbirler alarak,
    - Bilgi güvenliği, virüsler ve kötücül kodlar da dâhil üyeler arasında bilgi paylaşımını ve teknoloji değişimini kolaylaştırarak,
    - Üyeleri ilgilendiren konularda ortak araştırma ve geliştirme yapılmasını desteklemek,
    - Siber olaylarla etkin mücadele için bölgedeki diğer STİM'lere yardım ederek,

arttırmak
yer almaktadır.

EuroCERT hizmetleri ve APSIRC projesi ilgisizlikten ve mali yetersizlikten dolayı 1999 yılında sona ermiştir. İlerleyen zamanlarda yapılan çeşitli toplantıların sonucunda APSIRC projesi ile bir araya gelen grubun TERENA bünyesinde kurulan TF-CSIRT görev gücü adı altında çalışmalarına devam etmeleri kararlaştırılmıştır.

Avrupa'daki STİM'ler arasında işbirliğini teşvik eden bir yapı olan TF-CSIRT görev gücünün ana hedefleri (ENISA, 2006a):

- Deneyimlerin ve bilgilerin paylaşılması için bir forum sağlamak,
- Avrupa'daki STİM topluluğu için pilot hizmetler oluşturmak
- Güvenlik olaylarına karşı koymak için ortak standartların ve prosedürlerin teşvik edilmesi,
- Yeni STİM'lerin kurulmasına ve STİM personelinin eğitilmesine yardımcı olmak,

olarak sayılmaktadır (ENISA, 2006a).

c. Uluslararası işbirliği

Siber olaylarla mücadelede başarının en önemli anahtarlarından birinin farklı ülkelerdeki STİM'lerin işbirliği kurmaları olduğu ifade edilmektedir. Uluslararası işbirliğinin kurulması, internetin ve siber tehditlerin yayılmalarının doğası gereği bir zorunluluk olarak telaffuz edilmektedir. Bunun yanı sıra birçok diğer STİM hizmetinin sunulmasında da dünyanın farklı yerlerindeki STİM'lerle işbirliği kurulmasına ihtiyaç duyulduğu görülmektedir (ENISA, 2006b).

Uluslararası işbirliğinde öne çıkan en önemli birliğin FIRST olduğunu söylemek mümkündür. Özellikle FIRST bünyesinde kurulan özel ilgi gruplarının başarılı çalışmalar yürüttükleri ifade edilmektedir.

Devlet, ticari ve eğitim alanındaki çeşitli STİM'leri bir araya getiren uluslararası bir STİM topluluğu olan FIRST, siber olaylar karşısında hızlı tepki verilmesini sağlamak ve teşvik etmek amacıyla güvenlik olaylarının önlenmesinde işbirliği ve koordinasyon sağlamayı amaçlamaktadır. Üyeleri ve diğer STİM toplulukları arasında bilgi paylaşımının teşvik edilmesi de FIRST'ün hedefleri arasında yer almaktadır (ENISA, 2006a).

Uluslararası işbirliklerinde sektör tabanlı işbirliklerinin kurulduğu da görülmektedir. Sektör tabanlı uluslararası işbirliğinin hem kamu hem de özel sektörde kurulması mümkündür.

Avrupa'daki Kamu-STİM'lerin bir araya gelerek kurdukları bir grup olan Avrupa Devlet STİM'leri (European Government CSIRTs - EGC) bu bağlamda kurulan resmi olmayan bir gruptur. EGC'nin üyeleri arasında, siber olaylara müdahalede, benzer müşteri yapılarının oluşturulmasında ve ortak problemlerde etkin işbirliğinin sağlanması gibi amaçları bulunmaktadır (ENISA, 2006a).

EGC'nin üyeleri arasında; Fransa (CERTA), Almanya (CERT-Bund), Finlandiya (CERT-FI), Hollanda (GOVCERT.NL), İsveç (SITIC), İngiltere (UNIRAS), Norveç (NorCERT), İsviçre (SWITCH CERT) yer almaktadır (ENISA, 2006a).

1.3.4.5. İşbirliğinin sağladığı yararlar

STİM'ler arasında kurulan işbirliğinin tüm tarafların yararına bir girişim olduğunu söylemek mümkündür. Zira bir siber olayın işbirliği olmadan etkin bir şekilde bertaraf edilmesinin mümkün olmadığı herkes tarafından kabul gören bir gerçektir.

Siber olaylarla mücadelede tarafların sağladıkları faydaların, siber olayların ele alınması, proje yönetimi, kaynak ve bilgi paylaşımı ve sosyal ağ kurma alanlarında sağladıkları yararlar şeklinde dört alanda ele alındığı görülmektedir.

a. Siber olayların ele alınmasına ilişkin yararlar

Senelerce STİM'ler arasında kurulan işbirliklerin çıkarılan en önemli sonuçlardan birinin, siber olayların ele alınmasındaki gelişme olduğu vurgulanmaktadır. STİM'lere raporlanan siber olayların tamamına yakınının uluslararası boyutları olan siber olaylar olduğundan hareketle, siber olaylarla etkin bir şekilde mücadele etmek ve sonuç almak için tüm tarafların iyi bir işbirliği kurmaktan başka seçeneklerinin olmadığını söylemek mümkündür (ENISA, 2006b).

Olaya müdahale sürecinde taraflar arasında paylaşılan bilgilerin çok hassas ve önemli bilgiler olduğu, olayı bertaraf etmede ve oluşabilecek zararların asgari seviyede tutulmasında paylaşılan bu bilgilerin katkısının küçümsenemeyeceği ifade edilmektedir. Siber olayların raporlarının internetteki yasadışı grupların faaliyetleri, saldırılan organizasyonlar, siber suçluların planları, kötücül kodlara ilişkin detaylı analizler, elektronik deliller ve daha başka kritik öneme sahip bilgileri içerdiği düşünüldüğünde, bu bilgilerin güvenli yollarla taraflar arasında paylaşılmasının önemi de ortaya çıkmaktadır. Dolayısıyla siber olaylarla mücadelede işbirliğinin hayati önemde olduğunu söylemek mümkündür (ENISA, 2006b).

İşbirliği sürecinde paylaşılan kaynakların ve bilgilerin STİM'lerin ilgili müşterileri ile de paylaşılması durumunda, siber olaylarla mücadele sürecinin çok daha kaliteli bir şekilde yapılması mümkün olabilmektedir. Buna paralel olarak STİM'lerin iş yükünün de önemli miktarda azalacağı düşünülmektedir (ENISA, 2006b).

b. Proje yönetimine ilişkin yararlar

İşbirliğinin bir diğer sonucu olarak ortak projelerin yürütülmesi gösterilmektedir. STİM'ler arasında kurulan işbirlikleri, takımların kendi ilgi alanlarını, yeteneklerini, hedeflerini daha iyi fark etme ve güven tesis etme konularında olanaklar sunmaktadır. Bunun sonucu olarak da bazı takımların daha yakın işbirliklerine giriştikleri görülmektedir. Bu yakın işbirliğinin mevcut bir işbirliğinin bir parçası olması ya da tamamen yeni bir işbirliği projesi de olabilmektedir. TERENA TF-CSIRT işbirliğinin üyelerinden olan yedi STİM'in bir araya gelerek eCSIRT.net projesini hayata geçirmeleri bu konuda gösterilen örnekler arasında yer almaktadır. Söz konusu yedi STİM'in Trusted Introducer tarafından akredite edildiği ve yüksek bir güven seviyesine ulaştıkları bilinmektedir (ENISA, 2006b).

c. Kaynak ve bilgi paylaşımına ilişkin yararlar

Bilgi paylaşımını kaynakların paylaşılması veya STİM tarafından sunulan hizmetler olarak da düşünmek mümkündür. STİM'ler arasında paylaşılabilecek çeşitli kaynaklardan bahsedilebilir (ENISA, 2006b):

- Bilgi ve tecrübe paylaşımı
- Personel değişimi ve
- Teknoloji paylaşımı.

d. Sosyal ağ kurmaya ilişkin yararlar

STİM'ler arasında güvenilir bir ilişkinin kurulmasında sosyal ağ önemli bir faktör olarak değerlendirilmektedir. Kurulan sosyal ağ sayesinde STİM çalışanlarının bir araya gelerek birbirlerini daha iyi tanımaları ve bilgi paylaşımında bulunmaları mümkün olabilmektedir. Sosyal ağda kurulan işbirliklerinin genellikle daha yakın ve resmi işbirliklerinin doğmasına yardımcı olduğuna inanılmaktadır (ENISA, 2006b).

e. İşbirliğinin STİM hizmetlerine etkisi

STİM'ler arasında kurulan işbirliklerinin sunulan hizmetlerin gelişmesine etkisi (Tablo 1.11) işbirliği girişimlerinin en somut sonucu olarak değerlendirmek mümkündür. Zira yaşanan tecrübeler ve edinilen bilgiler doğrultusunda gelişmiş hizmetlerin sunulması ile siber olaylarla mücadelenin da daha etkin olabileceği değerlendirilmektedir (ENISA, 2006b).

Tablo 1.11. İşbirliği ile STİM hizmetlerinin kalitesi arasındaki ilişki

Hizmetler	**İşbirliğinin etkisi**		
	Düşük	**Orta**	**Yüksek**
Alarmlar ve Uyarılar	**Y**		**X**
Siber Olayların Ele Alınması		**Y**	**X**

Açıklıkların Ele Alınması	**Y**	**X**	
Saldırgan Araçların Ele Alınması	**Y**	**X**	
Teknoloji Takibi			**YX**
Güvenlik Araçlarının Konfigürasyonu ve bakımı	**Y X**		
Güvenlik Araçlarının Geliştirilmesi		**YX**	
Saldırı Tespit Hizmetleri	**Y**	**X**	
Risk Analizi	**YX**		
Farkındalık Oluşturma		**YX**	
Eğitim / Kurs		**YX**	
Ürün Değerlendirme ve Belgelendirme		XY	
X: İyi tasarlanmış işbirliği ile yakalanabilecek kalite seviyesi **Y:** Mevcut durumdaki kalite seviyesi			

Kaynak: (ENISA, 2006b)

Birçok STİM hizmetinin işbirliği sayesinde mevcut durumdakinden daha iyi bir kalite seviyesinde sunulabileceğine inanılmaktadır. Örneğin alarm üretme ve uyarı yayımlama hizmetinin farklı takımlar tarafından kullanılan ortak bir tavsiye formatının ve ortak tehdit değerlendirme standartlarının olması ile daha etkin bir şekilde sunulabileceği ifade edilmektedir (ENISA, 2006b).

1.3.4.6. İşbirliğinin önündeki engeller

Farklı STİM'lerin olması ve bunlar arasında bir işbirliğinin kurulması siber olaylarla mücadelede gelişmeyi sağlayan önemli parametreler arasında sayılmaktadır. STİM toplulukları ile iletişime geçmeye bazı STİM'ler ile işbirliği kurarak başlamak uygun bir yöntem olarak değerlendirilmektedir. Belirli bir tecrübe düzeyinde olan STİM'lerin genellikle yeni kurulan STİM'lere yardım etme eğiliminde oldukları da ifade edilmektedir (ENISA, 2006a).

İşbirliğinin taraflara birçok yararlar sağladığını söylemek mümkündür. Ancak işbirliği kurulmasını sınırlayan hatta bazı durumlarda imkânsız kılan bazı engellerden de bahsetmek mümkündür. Bu engellerin en önemlileri arasında;

- Standartlara uyulmaması,
- Mali konular,
- Servis seviyesi anlaşmasının olmaması,
- Hukuk sistemleri arasındaki farklılıklar ve
- Yeterli örgütsel ve politik desteğin olmaması

sayılmaktadır (Silicki ve Maj 2008).

Tespit edilen bu engellerin aşılması söz konusu olabilmektedir. Diğer taraftan bazı engellerin STİM dünyasında koyulan bazı çok önemli kuralların sonucu olduğu ve bu engellerin ortadan kaldırılması için yeterli imkânların olmadığı ifade edilmektedir (ENISA, 2006b).

a. Güven gereksinimi

Siber olayların ele alınması sürecinde STİM'ler gizlilik arz eden çok miktardaki hassas bilgilerle çalışmaktadırlar. Çoğu durumda bu bilgilerin işlenmesi ve kullanılması yasalarla düzenlenmektedir. Dolayısıyla bu düzenlemeler söz konusu bilgilerin paylaşılmasına ve farklı amaçlarla kullanılmasına birçok sınırlamalar getirmektedir. Ulusal bağlamda sorun teşkil eden bu konunun uluslararası işbirliklerinde de ciddi sorun teşkil ettiği ifade edilmektedir. Birçok STİM'in hassas bilgileri diğer STİM'lerle paylaşmasına izin verilmemektedir. Bu gibi durumlarda bilgilerin kısaltılarak anonimleştirilmesinden sonra paylaşılması söz konusu olmaktadır. Daha önce de bahsedildiği gibi kısaltılarak bir şekilde arındırılan bilgilerin işlenmesi STİM'lerin iş yükünü önemli oranda arttıran bir nedendir (ENISA, 2006b).

b. Mali konular

Daha yakın işbirliği kurulması mali giderleri önemli ölçüde arttırmaktadır. Ancak, elektronik posta veya elektronik ortamdaki paylaşım platformları aracılığıyla gerçekleştirilen temel seviyedeki işbirliğinde maliyetler düşük olmaktadır.

Dolayısıyla değeri olan bir işbirliğinin kurulmasının büyük oranda mali bir konu olduğu görülmektedir. Her ne kadar işbirliğinin taraflar arasındaki güvene dayalı olduğu ifade edilmiş olsa da gerçekte işbirliğinin kurulması için kişilerin birbirleriyle temasına ihtiyaç duyulmaktadır. Dolayısıyla işbirliği kurulmasında paranın bir engel olması söz konusu olmaktadır (ENISA, 2006b).

c. İşbirliğinde servis seviyesi anlaşmasının olmaması

Servis seviyesi anlaşmasının (SLA) olmaması daha çok takım-takım işbirliği modelinde problemlere yol açmaktadır. Taraflar arasındaki işbirliğini tamamen ortadan kaldırmayan bu eksikliğin süreci yavaşlattığına inanılmaktadır. SLA'nın siber olayların ele alınması sürecinde özellikle de talep ve yanıt sürelerinde sorun olduğu ifade edilmektedir. STİM dünyasında müşteriler dışındaki taraflardan yapılan taleplere yanıt süresi belirleme gibi katı kuralların belirlenmesinin çok yaygın olmadığı ve işbirliği için bir yarar da sağlamadığı düşünülmektedir. Bir SLA ile kurulan STİM işbirliğine pek rastlanmadığı ifade edilmektedir (ENISA, 2006b).

d. Hukuk sistemleri arasındaki farklılıklar

Dünyanın farklı yerlerindeki STİM'ler farklı yasal şartlar altında hizmet vermektedirler. Dolayısıyla hizmet verdikleri ülkedeki hukuki sistemin gereklerini yerine getirmeleri gerekmektedir. Bu problemin hizmetlerin sunulma şeklini etkilediğini söylemek mümkündür. Örneğin STİM bünyesinde oluşturulan verilerin nasıl, ne zaman ve kimlerle paylaşılabileceği ilgili ülkenin hukuk yapısına bağlı olarak değişiklik göstermektedir. Bu durumun bazı belirli siber saldırıların farklı ülkelerde farklı değerlendirilmesine neden olduğu ifade edilmektedir. Hukuk sistemindeki farklılıklar daha çok uluslararası işbirliklerini etkilemektedir (ENISA, 2006b).

e. Yeterli örgütsel ve politik desteğin olmaması

STİM'lerin büyük organizasyonel yapıların içinde yer alan bir birim olduğu düşünüldüğünde, büyüklükten kaynaklanan bir sonuçla yeteri kadar önemin

verilmediği görülmektedir. Dolayısıyla ana organizasyon tarafından gerekli desteğin gösterilmemesi söz konusu olmaktadır. Bu durumun sadece işbirliği kurulmasında değil STİM'in gelişmesinde de problem teşkil ettiği ifade edilmektedir. Yeterli örgütsel desteğin verilmemesinin bir diğer nedeni olarak rakiplerle kurulacak işbirliğinin rekabeti olumsuz etkilemesi endişesi olarak gösterilmektedir. Aslında herhangi bir sektördeki STİM'lerin işbirliği içinde çalışmalarının rekabet açısından da gerekli olduğunu söylemek mümkündür. Zira bu tarz bir işbirliğinde hem rakiplerle yakın bir çalışma ortamı hem de siber olaylarla etkin mücadele edilmesi söz konusudur. STİM çalışanlarının işbirliğinin gerekliliği ve organizasyona sağlayacağı yararlar konusunda yöneticilerini bilgilendirmeleri önerilmektedir. Örgütsel ve politik desteğin mali yansımalarının da olması gerektiği ifade edilmektedir (ENISA, 2006b).

f. Standartlara uyulmaması

İlk STİM yaklaşık 24 yıl önce kurulmuş olmasına rağmen henüz STİM süreçleri için tanımlanmış bir standardın bulunmadığı ifade edilmektedir. Ancak STİM'lerden beklentiler konusunda bir yorum talebi (Request For Comment - RFC) gibi çeşitli dokümanlar bulunmaktadır. Standartların olmamasının STİM hizmetlerine ve süreçlerine çeşitli etkileri söz konusu olmaktadır (Tablo 1.12) (ENISA, 2006b).

Tablo 1.12. Eksik veya yaygın olarak benimsenmeyen standartların etkisi

Eksik ya da yaygın olarak benimsenmemiş standart	**Muhtemel sonuçları**
Siber olayların sınıflandırılması	• Ortak istatistiklerin olmaması • Belirsiz tehdit değerlendirmesi • Bir olgu değerlendirme ölçeğinin imkânsızlığı
Veri değişim formatı	• Önemli verinin gecikmeli olarak değişimi • Siber olay verilerinin işlenmesinin ve siber olayların ele alınmasının otomatik yapılmasında zorluk

Siber olayların ele alınması işlemi	• Tepki zamanının bilinmemesi • Sorun çözme zamanının bilinmemesi • İşlem sırası takibinin bilinmemesi
Siber olay raporlarının içeriği (Saldırganın IP adresi, mağdurun IP adresi, işletim sistemi günlük kayıtları vb.)	• Sorunun çözümü için önemli olan bazı verilerin eksikliği
Güvenlik önerilerinin formatı	• Mevcut önerilerin kullanılması yerine yeni önerilerin hazırlanması ile ek iş yükü olması • Tehditlere gecikmiş tepkilerin verilmesi
Tehdit değerlendirmesi (genel açıklık puanlama sistemi)	• Yönetimin kararını değiştirmenin zorluğu • Gerektiğinde çözüm konfigürasyonunda değişiklik yapılamaması

Kaynak: (ENISA, 2006b)

2. U-STİM'İN İŞLEYİŞİNE İLİŞKİN DÜNYA UYGULAMALARI

Siber tehditlerin artmasıyla birlikte dünya üzerindeki ülkelerde hemen her gün yüzlerce siber olay meydana gelmektedir. Devletler, vatandaşlarını, kurumlarını ve ülkelerini siber tehditlerden ve siber olaylardan korumak, siber güvenliğin sağlanmasına katkıda bulunmak amacıyla çeşitli çalışmalar yürütmektedirler. U-STİM yapılarının oluşturulması ve siber tehditlerle mücadele hizmeti vermesi yürütülen bu çalışmalar arasında yer almaktadır. Bu bölümde ABD, Hollanda, Avustralya ve Çin'de kurulan U-STİM yapıları yüklendikleri misyon, sundukları hizmetler, hizmet sundukları müşteriler ve yürüttükleri diğer faaliyetler bağlamında incelenmektedir.

2.1. ABD (US-CERT)

2003 yılında ABD ulusunun internet altyapısını korumak üzere kurulan ve ülkede siber saldırılara karşı verilen savunmaları ve karşı koymaları koordine eden ABD U-STİM'i (United State CERT - US-CERT), İç Güvenlik Bakanlığı (Department of Homeland Security - DHS) ile kamu ve özel sektör arasındaki bir işbirliği organizasyonudur. Merkezi Washington'da bulunan US-CERT, DHS bünyesindeki Ulusal Siber Güvenlik Birimi'nin (National Cyber Security Division - NCSD) operasyonel kolu olarak faaliyet göstermektedir. US-CERT ayrıca, federal ajanslarla, merkezi ve yerel hükümetlerle, uzmanlarla ve diğer ilgililerle etkileşimde bulunarak bilgi paylaşımının ve olaylara müdahale koordinasyon yeteneğinin geliştirilmesini ve dolayısıyla da siber tehditlerin ve güvenlik açıklarının azaltılmasını hedeflemektedir (US-CERT, 2008).

Siber olaylara müdahale ile ilgilenen dünya çapında 250 den fazla organizasyon bulunmaktadır. US-CERT bu gruplardan bağımsız olduğunu söylemekle birlikte siber olaylar konusunda bu gruplarla koordine olabileceğini ifade etmektedir. Bu tür organizasyonların ilki olan CERT/CC 1988 yılında ABD'de Carnegie Mellon Üniversitesi'nde kurulmuştur. US-CERT DHS tarafından kurulduğunda CERT/CC'ye, siber saldırılara karşı koymak ve koordinasyon içinde ülkenin altyapısını korumak amacıyla uzman olarak katkıda bulunması çağrısında

bulunulmuştur. DHS ve CERT/CC US-CERT aracılığıyla siber tehdit konularda birlikte çalışmaktadırlar (US-CERT, 2011).

2.1.1 Misyonu

US-CERT DHS tarafından kurulmuştur ve siber uzaydaki olayların analiz edilmesi, siber güvenlik uyarılarının yapılması, bilgi paylaşımı ve olaylara müdahale ve geri kurtarma süreçlerini geniş bir kullanıcı yelpazesi için yönetmek ve koordine etmek üzere yegâne temas noktası olarak ve 7/24 hizmet vermektedir. US-CERT, devlet, kurumlar, küçük işletmeler ve ev kullanıcılarından oluşan bir kullanıcı kitlesine hizmet vermektedir.

US-CERT, ulusun internet altyapısının güvenliğini sağlamak ve ülkede siber saldırılara karşı yapılan savunmaları koordine etmek üzere DHS ile kamu ve özel sektör arasında kurulan bir işbirliğidir (DHS, 2009).

US-CERT;

- Siber tehditlerin ve güvenlik açıklarının analiz edilmesi ve azaltılması,
- Siber tehditler konusunda uyarıcı bilgilerin yayımlanması,
- Siber olaylara müdahale çalışmalarının koordine edilmesi

konularından sorumludur (DHS, 2009)

2.1.2 Verdiği hizmetler

US-CERT aşağıda yer alan hizmetleri ve destekleri sunmaktadır:

- Federal, kamu ve özel sektöre ve uluslararası topluma 24x7x365 güvenlik olaylarını sınıflandırarak öncelik/sonralık saptaması desteği vermek,
- Siber güvenlik olaylarını izlemek ve öngörü analizleri yapmak,
- Ortaya çıkan tehditler için gelişmiş uyarı,
- Federal ve devlet kurumları için olaylara müdahale imkânları,
- Kötücül yazılım analizi ve geri kurtarma desteği,
- Eğilimler ve raporlama araçlarının analizi,

- Ulusal ve uluslararası seviyede tatbikatlar yapmak ve bu tatbikatlara katılmak (US-CERT, 2009)

Bunların yanında US-CERT tarafından aşağıdaki başlıklar altında da çalışmalar yapılmaktadır:

Siber güvenlik bültenleri: Sistem yöneticileri ve teknik kullanıcılar için yazılan bu materyaller yeni güvenlik problemleri ve açıkları ile ilgili yayımlanan bilgileri özet halinde sunmaktadır.

Teknik siber güvenlik alarmları: Sistem yöneticileri ve deneyimli kullanıcılar için üretilen teknik alarmlar mevcut güvenlik sorunlarına, açıklarına ve istismarlara ilişkin güncel bilgiler sağlamaktadır.

Siber güvenlik alarmları: Ev kullanıcıları, kurumsal bireysel kullanıcılar ve yeni kullanıcılar için hazırlanan bu tür alarmlar toplumun genelini etkileyen bir güvenlik sorunu olduğunda teknik alarmlar ile birlikte yayımlanmaktadır.

Siber güvenlik ipuçları: Ev kullanıcıları, kurumsal bireysel kullanıcılar ve yeni kullanıcılara daha çok hitap eden ipuçları, çeşitli genel güvenlik sorunlarına ilişkin bilgi ve tavsiyeler içermektedir. İpuçları, toplumun genelini etkileyen bir güvenlik sorunu olduğunda teknik alarmlar ile birlikte iki haftada bir yayımlanmaktadır.

Ulusal İnternet Yayın Girişimi: DHS, US-CERT ve çok uluslu bilgi paylaşım ve analiz merkezleri ile siber güvenlik sorunlarının ele alınacağı bir dizi internet yayını geliştirmek amacıyla bir ortaklık başlatmıştır. Girişimin amacının ulusun siber olaylara karşı hazırlıklı olmasını sağlamak ve dayanaklılığını arttırmak olarak ifade edilmektedir (DHS, 2009)

2.1.3 Hizmet verdiği kurum/kuruluşlar

US-CERT'in; siber olaylara müdahale etmek, mağdurlara teknik destek vermek, federal sivil yürütme organlarını (.gov) siber saldırılara karşı savunmak, bilgi

paylaşımını sağlamak ve uluslararası ortaklarla işbirliği çalışmalarını yürütmek gibi görevleri bulunmaktadır (US-CERT, 2008).

Ayrıca vatandaşlara, iş dünyasına ve diğer kurumlara siber güvenlik konusunda doğrudan ABD hükümeti ile iletişime geçme imkânı ve bunu koordine etme hizmeti de vermektedir (US-CERT, 2011).

2.1.4 Faaliyetleri

US-CERT 2009 yılının ilk çeyreği için siber güvenlik eğilimlerini belirlemiş ve bunu bir rapor olarak yayımlamıştır (US-CERT, 2009). Çalışma esnasında Tablo 2.1'de yer alan kategorilerde inceleme yapılmıştır.

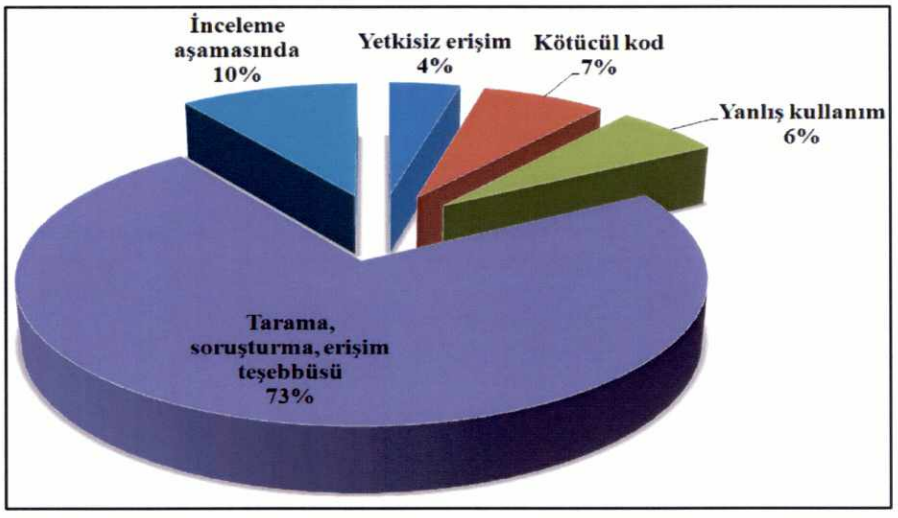
Tablo 2.1. US-CERT -2009 ilk çeyrek raporunda incelenen kategoriler

Kategori	Açıklama
KATEGORİ 1 Yetkisiz Erişim	Bu kategoride bir kişi bir federal ajans ağına, sistemine, uygulamasına, verisine veya başka bir kaynağına izinsiz fiziksel veya mantıksal erişim elde etmesi incelenmiştir.
KATEGORİ 2 DoS	Kaynakları tüketerek ağların, sistemlerin veya uygulamaların normal çalışmasını engelleyen veya bozan bir saldırı DoS. Bu inceleme kategorisi DoS saldırısının mağduru olmayı veya böyle bir saldırıya karışmış olmayı da içermektedir.
KATEGORİ 3 Kötücül Yazılım	Kötücül yazılımların başarılı bir şekilde yüklenmesi.
KATEGORİ 4 Kötü Kullanım	Kişinin kabul edilebilir bilgisayar kullanım politikalarını ihlal etmesi.
KATEGORİ 5 Taramalar, Yoklamak veya Erişim Teşebbüsü	Federal ajansın bir bilgisayarını, açık portlarını, protokollerini, hizmetlerini tespit etmek veya bunlara erişmek isteyen herhangi bir faaliyet. Böylesi bir faaliyetin sonucu her zaman ele geçirme veya servis dışı bırakma olmamaktadır.
KATEGORİ 6 Soruşturma	Potansiyel olarak kötücül veya anormal faaliyetlerin doğrulanmamış olayların raporlama birimi tarafından daha detaylı incelenmesi.

Kaynak: US-CERT

Şekil 2.1'de siber güvenlik olaylarının Tablo 2.1'deki kategoriler arasındaki dağılımını göstermektedir.

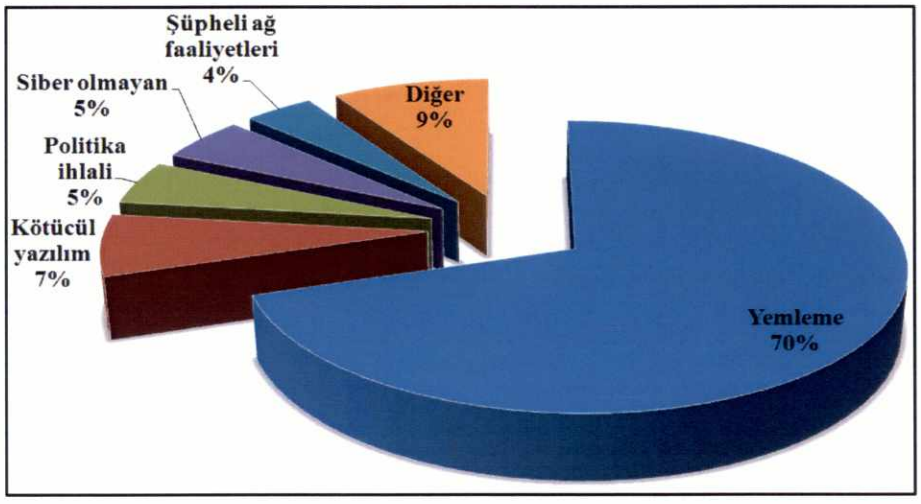
Şekil 2.1 US-CERT -2009 ilk çeyrek raporundaki olay kategorileri



Kaynak: (US-CERT, 2009)

Şekil 2.2'de sıralamada ilk beşe giren olayların meydana gelme oranları verilmektedir. Bildirilen tüm olaylar içindeki oranına bakıldığında yemlemenin en yaygın olay olarak kalmaya devam ettiği görülmektedir (US-CERT, 2009)

Şekil 2.2 US-CERT -2009 ilk çeyrek raporuna göre en çok görülen 5 olay



Kaynak: (US-CERT, 2009)

2.2. Hollanda (GOVCERT.NL)

2002 yılında Hollanda hükümeti tarafından CERT-RO adıyla kurulan, adı 2003 yılında GOVCERT.NL olarak değiştirilen ve Hollanda'nın U-STİM'i olan GOVCERT.NL, siber olayların önlenmesi ve bu olaylara müdahalenin koordine edilmesi amacıyla çalışmalar yürütmekte ve müşterilerine siber olaylarla mücadele konusunda hizmet sunmaktadır (GOVCERT.NL, 2010).

İçişleri ve Kraliyet İlişkileri Bakanlığı bünyesinde yer alan GOVCERT.NL, olaylara karşı koyma, uzmanlık merkezi ve yeni servisler olmak üzere üç ekipten oluşmaktadır. İçişleri ve Kraliyet İlişkileri Bakanlığı bünyesindeki ilgili genel müdür GOVCERT.NL'nin komisyon üyesi olarak yer almaktadır (GOVCERT.NL, 2010).

Siber güvenliğe kapsamlı bir yaklaşım sergileyen ve hazırlanmasında GOVCERT.NL'nin aktif bir şekilde yer aldığı, Hollanda Ulusal Siber Güvenlik Stratejisi Güvenlik ve Adalet Bakanı tarafından 22 Şubat 2011 tarihinde kamuoyuna duyurulmuştur. Söz konusu stratejide ulusal siber güvenliğin sağlanmasında özel sektörle işbirliği kurulması ön plana çıkmaktadır. Strateji ile Siber Güvenlik Konseyi ve Ulusal Siber Güvenlik Merkezi (USGM) kurulması planlanmaktadır. Stratejide GOVCERT.NL'nin, kurulması planlanan USGM'nin bir parçası olarak hizmet vermesi önerilmektedir. Bu durum, GOVCERT.NL'nin USGM'de önemli bir rol alacağı şeklinde değerlendirilmektedir (GOVCERT.NL, 2011).

Stratejide, siber güvenliğin sağlanması konusundaki düzenlemelerde öz düzenlemenin benimsenmesi, öz düzenlemenin yetersiz kalması durumunda devlet düzenlemesi modelinin kullanılması önerilmektedir. Ancak kanuni düzenlemelerin, rekabeti bozucu olmamasına ve bir faaliyet alanı sağlamasına, idari yükün orantısız artışına yol açmamasına ve maliyet-fayda oranlarını makul seviyede tutmasına itina göstermesi istenmektedir (Hollanda, 2011).

2.2.1. Misyonu

GOVCERT.NL, kurulduğu 2002 yılından bu yana Hollanda devletine siber olayların önlenmesi konusunda destek vermektedir. Başlıca görevleri:

- Siber olaylarının meydana gelmesi durumunda ilgili taraflar arasında koordinasyonu sağlamak,
- Siber olayları önlemek için proaktif hareket etmek veya oluşabilecek siber olayları ve oluşabilecek zararları asgari seviyede tutmak için hazırlık yapmak

olarak tanımlanmaktadır (GOVCERT.NL, 2010)

2.2.2. Verdiği hizmetler

GOVCERT.NL müşterilerine dört ana başlık altında hizmet sunmaktadır:

- Siber olayları önleme kapsamında güvenlik duyuruları yayımlamak, güvenlik danışmanlığı yapmak, gerektiğinde alarm üretmek, eğitim vermek ve tatbikat düzenlemek.
- Siber olayları raporlamak, koordinasyonu sağlamak ve siber olaylara karşı koymak.
- Ağı haftanın yedi günü, günde oniki saat aktif olarak izlemek.
- Siber olaylara karşı koyma konusundaki en iyi uygulamaları paylaşmak, bültenler yayımlamak ve sempozyumlar düzenlemek suretiyle bilgi paylaşımında bulunmak (GOVCERT.NL, 2010).

GOVCERT.NL izleme, bilgi paylaşımı, siber olayların önlenmesi ve siber olaylara karşı koyulması alanlarında hizmet vermeye yoğunlaşmıştır:

- İzleme, siber tehditlerin ve güvenlik açıklarının güncel ve doğru bir haritasının ortaya koyulması için gerçekleştirilen bütün faaliyetleri kapsamaktadır. BİT sistemlerini ve altyapılarını hedef alabilecek yeni tehditlere karşı açık ve kapalı kaynaklar haftanın yedi günü on iki saat (7/12) GOVCERT.NL tarafından analiz edilmektedir. Ayrıca saldırılar hakkında operasyonel ve taktik bilgiler elde etmek için otomatik sensör sistemleri geliştirilmekte ve konuşlandırılmaktadır.
- Bilgi paylaşımı, STİM dünyasının ve STİM'lerden hizmet alan müşterilerin yeteneklerinin pekiştirilmesinde önemli bir etkiye sahiptir. Başarılı uygulamaların ve tehditlere ilişkin bilgilerin paylaşılması için bültenler ve tanıtım yazıları yayımlanmaktadır. GOVCERT.NL'nin iş süreçlerini kolaylaştırmak için

geliştirilen araçlar STİM dünyası ile paylaşılmaktadır. Bu bilgiler aynı zamanda Bilgi Paylaşımı ve Analiz Merkezleri (Information Sharing and Analysis Centers - ISACs) vasıtasıyla Hollanda'daki hayati öneme sahip organizasyonlar ile de paylaşmaktadır (GOVCERT.NL, 2010)

- Müşterilerin, bir siber olaya maruz kalma ihtimallerini veya meydana gelen bir olaydan uğrayacakları zararı azaltmak için önleme ve hazırlık çalışmaları yürütülmektedir. Bu kapsamda yeni tehditler ve işleyişi olumsuz etkileyebilecek saldırılar konusunda bilgiler sağlanmakta ve yapılabileceklere ilişkin tavsiyelerde bulunulmakta, personelin farkındalığını ve becerilerini arttırmak için çalışmalar yapılmaktadır (GOVCERT.NL, 2010).
- Siber olaylara karşı koyulması, BİT'lere ilişkin her türlü olayın ardından kurtarma çalışmalarının koordine edilmesi için, 7/24 erişilebilirlik hizmeti sunulmaktadır. Bu hizmet, siber olayın bertaraf edilmesi amacıyla harekete geçilmesini, analizler yapılmasını ve ilgili paydaşlarla ve medya ile haberleşilmesini kapsamaktadır (GOVCERT.NL, 2010).

GOVCERT.NL bu alanlarda ilave bazı hizmetler daha sunmaktadır:

- Uluslararası bilgi paylaşımı: BİT'lerin güvenliğinin sağlanmasının sınırları aşan bir konu olmasından yola çıkarak, GOVCERT.NL verdiği hizmetlerin kalitesini korumak için uluslararası seviyede bilgi paylaşımında ve işbirliğinde bulunmanın önemli olduğuna inanmaktadır. GOVCERT.NL'nin uluslararası geniş bir ağın parçası olması da bu ihtiyacın giderilmesine yönelik olarak atılan bir adım olarak görülmektedir.
- Veri bankası: GOVCERT.NL'nin bir bilgi bankası olduğu ifade edilmektedir. Taraflar bilginin paylaşılması konusunda teşvik edilmektedir (GOVCERT.NL, 2010).

GOVCERT.NL bünyesinde, yazılımlardaki ve sistemlerdeki tehditleri ve açıklıkları bulmak için interneti 7/24 tarayan bir ekip bulunmaktadır. Bu ekip tarafından elde edilen bilgiler ışığında çeşitli ürünler geliştirilmekte yayımlanmaktadır. Bu sürecin iş

akışına yardımcı olması amacıyla da Taranis adı verilen bir sistem geliştirilmiştir. Veri toplamak, bu verileri analiz etmek ve bunun sonucunda bilgiler yayımlamak amacıyla GOVCERT.NL tarafından geliştirilen bir uygulama olan Taranis, özel olarak STİM yapılarındaki iş akışı işlevini yerine getirmek üzere tasarlanmıştır. Uygulamanın geliştirilmesi aşamalarında izlenebilirliğe ve şeffaflığa çok önem verildiği ifade edilmektedir (GOVCERT.NL, 2011).

Her gün 900 kaynağın bu ekip tarafında incelenmekte, inceleme konusuna göre ilgili haberler ve e-postalar analiz edilmekte, bu çalışmalar sonucunda elde edilen bilgiler kullanılarak farklı seviyelerdeki okuyuculara ve müşterilere hitap eden bazı ürünler üretilmektedir (GOVCERT.NL, 2011).

Beş aşamalı bir iş akış mimarisi olan Taranis ile veriler beş aşamalı bir sürecin sonunda elde dilmekte ve zenginleştirilerek bilgiye dönüştürülmektedir. Sonrasında bu bilgiler ilgisine göre hedef kitleye hitap edebilecek ürünlere dönüştürülmektedir (GOVCERT.NL, 2011).

2.2.3. Hizmet verdiği kurum/kuruluşlar

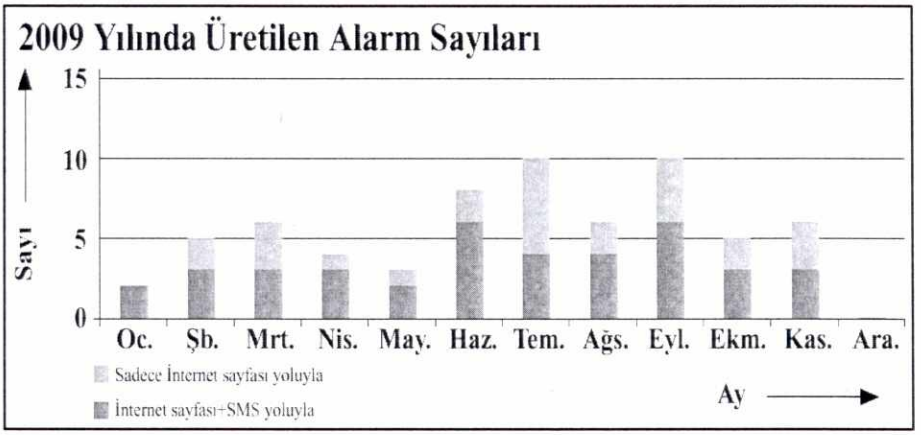
Kamu kurumları veya yüzde yüz kamu iştiraki olan özel kuruluşlar üyelik sistemi ile GOVCERT.NL tarafından sunulan hizmetlerden yararlanabilmektedir. Devlet tarafından karşılanan bir bütçeye sahip olan merkezi kamu kurumları hariç tüm üyelerin üyelik aidatı ödemesi zorunlu tutulmaktadır. Üye olmayan kurum/kuruluşların en iyi uygulama örneklerine ve bültenlere erişebilecekleri bir sayfa bulunmaktadır (GOVCERT.NL, 2010).

Güvenlik alarm merkezi (GAM) hizmeti www.waarschuwingsdienst.nl adresinden ücretsiz olarak isteyen herkese sunulmaktadır. Risklere ilişkin uyarıları e-posta veya mesaj olarak almak için söz konusu sayfaya kayıt olunması gerekmektedir (GOVCERT.NL, 2010).

2.2.4. Faaliyetleri

2009 yılının sonu itibariyle GOVCERT.NL tarafından e-posta veya KMS yoluyla 66.913 adet üyeye alarm, 27.685 adet üyeye ise aylık bülten gönderilmiştir. Yine aynı yılda 26 tanesi KMS ve e-posta yoluyla, 41 tanesi de internet sayfası aracılığıyla olmak üzere GAM üzerinden 67 adet alarm üretilmiştir (Şekil 2.3).

Şekil 2.3. GOVCERT.NL-2009'da GAM ile yayımlanan alarm sayıları



Kaynak: (GOVCERT.NL, 2009)

2009 yılında ele alınan siber olayların ve yemleme olayları için alınan önlemlerin aylara göre sayıları Tablo 2.2de yer almaktadır.

Tablo 2.2. GOVCERT.NL-2009 güvenlik olayları ve yemleme için önlemler

	2009 yılındaki güvenlik olayları		**Yemleme olayları için alınan önlemler**	
Ay	**Adet**	**Kümülâtif**	**Adet**	**Kümülâtif**
Ocak	5	5	3	3
Şubat	7	12	3	6
Mart	9	21	8	14
Nisan	17	38	3	17
Mayıs	3	41	1	18
Haziran	8	49	5	23
Temmuz	14	63	1	24

Ağustos	11	74	3	27
Eylül	6	80	0	27
Ekim	5	85	1	28
Kasım	9	94	2	30
Aralık	8	102	7	37

Kaynak: (GOVCERT.NL, 2009)

Aralarında ABD, İngiltere, Avustralya, Kanada, Almanya, Fransa, Japonya, Hollanda'nın bulunduğu toplam 15 ülkeyi içine alan ve gayrı resmi bir işbirliği girişimi olan Uluslararası İzleme ve Uyarma Ağı (International Watch and Warning Network - IWWN) aracılığıyla 2008 yılında bir tatbikat gerçekleştirilmiş, söz konusu tatbikat GOVCERT.NL tarafından organize edilmiştir. IWWN bünyesinde Hollanda'yı STİM olarak GOVCERT.NL temsil etmekte ve bu işbirliği girişimi içinde Hollanda'nın ulusal temas noktası olarak yer almaktadır. Ulusal ve uluslararası seviyede düzenlenen tatbikatların kötücül faaliyetlere karşı hazırlıklı olmak için önemli olmasından hareketle, GOVCERT.NL IWWN bünyesinde gerçekleştirilen tatbikatlara katılmaya önem vermektedir (GOVCERT.NL, 2009)

IWWN'de sırayla katılımcı her ülke bir tatbikat organize etmekte ve tatbikatın koordinasyonunu sağlamaktadır. Hollanda tarafından koordine edilen 2008 yılındaki tatbikatın amacı, bir kriz anında katılımcı organizasyonların erişilebilirliğinin test edilmesi olarak belirlenmiştir. Bunu uygulamak amacıyla tatbikatta, önceden herhangi bir uyarıda bulunmaksızın çeşitli kanallardan bir mesaj gönderilmiş ve bu mesaja 24 saat içinde cevap verilmesi beklenmiştir. Elde edilen sonuçlar testin önemini vurgulamıştır. Zira bütün tarafların hızlı ve etkili bir şekilde cevap dönmedikleri tespit edilmiştir (GOVCERT.NL, 2009)

GOVCERT.NL, başka uluslararası tatbikatlarda da gerek tatbikatların hazırlanmasında uzman olarak gerekse kötücül faaliyetlere cevap veren oyuncu devlet olarak sık sık yer almaktadır. Ulusal ve uluslararası temelde farklı kurum ve özel sektör ilgililerinin bir araya getirilmesinin ve bir kriz meydana geldiğinde cevap vermeye birlikte hazır olmanın tek yolunun tatbikatlar düzenlemek olduğuna inanılmaktadır (GOVCERT.NL, 2009)

GOVCERT.NL, Surfnet ve Polonya U-STİM'i, bir tarayıcı vasıtasıyla bilgisayarlara kötücül yazılım bulaştırmaya çalışan şüpheli internet sayfalarını arayan bir araç geliştirmişlerdir. ***HoneySpider*** Ağ Aracı adındaki bu yazılımın ilk sürümü 2010 yılında çıkmıştır. Çok sayıda internet sayfasının test edilmesine olanak sağlayan ve böylece güvenlik çalışanlarının iş yükünü önemli ölçüde azaltan bu yazılımın test çalışmalarına uluslararası STİM'ler ve güvenlik grupları destek vermektedir (GOVCERT.NL, 2009).

Yine 2009 yılında kötücül yazılımların analiz edilmesi ve bu konuda işbirliğinin teşvik edilmesi amacıyla bazı Avrupa STİM'lerinin katılımıyla bir kötücül yazılım laboratuarı çalıştayı düzenlenmiş, söz konusu çalışmaların sonucunda, kötücül yazılımların elde edilmesi ve analizi için bir altyapının kurulması ve hayata geçirilmesi çalışmaları başlatılmıştır (GOVCERT.NL, 2009).

2009 yılında gerçekleştirilen faaliyetlere bakıldığında GOVCERT.NL tarafından (GOVCERT.NL, 2009):

- Toplamda 8.760 saat erişilebilir olunmuş ve müşterilere kesintisiz hizmet verilmiş,
- 777 adet güvenlik alarmı gönderilmiş,
- GAM üzerinden 67 adet alarm yayımlanmış,
- 8 organizasyon Taranis sistemi ile çalışmış,
- 6 organizasyon HoneySpider aracını kullanmak için centilmenlik anlaşması imzalamıştır.

2.2.5. Ulusal ve uluslararası ortaklıklar

Ulusal bağlamda GOVCERT.NL, ulusal polis, istihbarat servisi, siber suçlara karşı ulusal altyapılar, Hollanda telekom otoritesi, Hollanda'daki internet servis sağlayıcılar ve yine Hollanda'daki diğer olaylara müdahale ekipleri ile birlikte çalışmaktadır. Yemleme sayfaları ile mücadele edilmesinde ise bankacılık sektörü ile yakın işbirliği içinde oldukları belirtilmektedir (GOVCERT.NL, 2009).

Uluslararası bağlamda ise GOVCERT.NL'nin, özellikle Hollanda dışındaki diğer STİM'lerden ve uluslararası organizasyonlardan oluşan geniş bir ağın parçası haline gelerek çalışmalarına ülke sınırlarını aşan bir boyut kazandırdığı görülmektedir. Kıt imkânlarla büyük sonuçlar elde etme amacında olduğunu ifade eden GOVCERT.NL, bunu gerçekleştirmenin yollarından birinin uluslararası işbirliği olduğuna inanmaktadır. GOVCERT.NL'nin dâhil olduğu uluslararası ağlar arasında aşağıda sıralanan kuruluşlar yer almaktadır (GOVCERT.NL, 2009):

- EGC: GOVCERT.NL'nin önemli bir konuma sahip olduğu EGC, coğrafi olarak Avrupa bünyesinde bulunan hükümetler için çalışan 10 STİM'in bir araya gelmesi ile oluşturulmuş bir işbirliği platformudur. Üyeler bir Kamu-STİM olarak en iyi işleyişin ne olduğu ve bu yeteneğin nasıl elde edilebileceği konusunda operasyonel ve pratik anlamda karşılıklı görüş alış verişinde bulunmaktadırlar. Bilgi paylaşımında gizliliğe çok önem verilmektedir. GOVCERT.NL, her yıl EGC toplantılarından birini düzenlemekte, EGC'nin alan adı kayıt işlemlerini yürütmekte, bir siber olay meydana geldiğinde kullanılan EGC temas listesinin güncellenmesi görevini de yürütmektedir.
- FIRST: Dünya çapında 238 STİM'in üyesi olduğu FIRST bünyesinde Ağ İzleme Özel İlgi Grubu (Aİ-ÖİG, Network Monitoring Special Interest Group - NM-SIG) GOVCERT.NL kurmuş ve grubun başkanlığını yürütmektedir. GOVCERT.NL ayrıca FIRST'e üye olmak isteyen yeni adaylara, rehberlik hizmetinin verildiği ve aday STİM'in tesislerine bir ziyaretin gerçekleştirildiği sponsorluk hizmeti vermektedir. Ziyaretin sonunda bir rapor hazırlanmakta ve bu rapor söz konusu STİM'in üyeliğinin kabul edilmesinde değerlendirilmektedir (GOVCERT.NL, 2009)
- Avrupa akademik ağların lobisi olan TERENA.
- Özel sektör katılımcılarını da kapsayan ve güvenlik alanında bir işbirliği olan Uluslararası Bilgi Bütünlüğü Enstitüsü (International Information Integrity Institute – I4)
- Çeşitli uluslararası kuruluşlardan oluşan ve güvenlik alanındaki işbirliklerinden biri olan Bilgi Güvenliği Forumu (Information Security Forum - ISF)

2.3. Avustralya (AusCERT)

Queensland üniversitesindeki kar amacı gütmeyen bir güvenlik grubu ve Avustralya'nın lider STİM'i olan AusCERT, Avustralya kamu kuruluşları, üyeleri ve yükseköğretim de dâhil olmak üzere müşterilerine siber saldırıların önlenmesi, tespit edilmesi, karşı koyulması ve azaltılması konularında destek sunmaktadır. Ayrıca AusCERT, küresel siber tehditleri ve açıklıkları izlemekte ve değerlendirmektedir. AusCERT Avustralya'yı etkileyen siber olayların çözümü için tek irtibat noktası olarak hizmet vermektedir (AusCERT, 2011).

AusCERT, üyelik aidatları, düzenlenen yıllık konferanslar ve hizmet sözleşmeleri gibi çeşitli kaynaklarla kendi kendini finanse eden ve işletim maliyetlerini karşılayan bir STİM'dir. Bundan başka Avustralya hükümetinin güvenli internet projesini (GİP, Stay Smart Online Alert Service) yürüten AusCERT proje kapsamında fonlanmaktadır (AusCERT, 2011).

FIRST'ün ve APCERT'in aktif bir üyesi olan AusCERT, Güney Amerika'dan, İngiltere'den, Avrupa'dan ve Asya'dan güvenilir STİM'lerden oluşan bir ağın yönetimini yürütmektedir. Söz konusu STİM'lerden, küresel tehditlere ilişkin uyarıları zamanında almalarını sağlamak, özellikle yargıya konu olan siber olaylara karşı koyulmasında yardım talep edilebilmektedir (AusCERT, 2011).

1993 yılında kurulan AusCERT dünyanın en eski STİM'lerinden biri olarak kabul edilmektedir. Kurulduğu günden 2010 yılına kadar Avustralya'nın U-STİM'i olarak 17 personelle hizmet veren AusCERT'in ulusal STİM görevini, 2010 yılında kurulan ve Avustralya hükümeti tarafından fonlanan CERT Australia devralmış, AusCERT'in CERT Australia'ya imzalanan bir sözleşme çerçevesinde hizmet vereceği belirtilmiştir (APCERT, 2009).

2.3.1 Misyonu

Avustralya'nın ve Asya-Pasifik bölgesinin öncü STİM'i olan AusCERT'in dünyanın dört bir yanından siber güvenlik uzmanlarından oluşan ve dünyaca tanınan, itibarlı ve

güvenilir bir ağ oluşturma misyonu bulunmaktadır. AusCERT, üyeleri için siber olaylardan korunma, siber olaylara karşı koyma ve siber tehditleri azaltma stratejileri üretme çalışmalarını:

- Hem ulusal hem bölgesel olarak bilgi paylaşımında bulunarak,
- Yerel ve küresel tehdit eğilimlerini takip ederek,
- Siber olaylara karşı koyarak ve karşı koymada destek vererek,
- Uluslararası STİM çalışmalarına liderlik yaparak,
- Gelişmiş siber güvenlik eğitimlerine öncülük yaparak ve
- Önde gelen güvenlik uzmanlarının tercih ettikleri işveren olarak

yürütmeyi amaçlamaktadır (AusCERT, 2011).

2.3.2 Verdiği hizmetler

AusCERT üyelerine:

- Kısa mesaj servisi ile uyarı ve alarm,
- Kötücül internet bağlantı adreslerini bildirme,
- Uzaktan görüntüleme,
- AusCERT tarafından yayımlanan bültenlerin yer aldığı ve sadece üyelerin erişimine açık internet sayfaları ve
- Siber olayların yönetimi

hizmetleri sunmaktadır (AusCERT, 2011).

a. Siber olayların yönetimi hizmetleri

Siber olayların koordine edilmesini ve ele alınmasını kapsayan siber olay yönetimi hizmeti öncelikle AusCERT üyelerine ve kamu kurumlarına sunulmaktadır. AusCERT'e üye olmayan organizasyonların yardım taleplerine ise mümkün olan en kısa sürede cevap verilmektedir. Dolayısıyla üyelik aidatı ödeyen kurum ya da kuruluşların önceliklendirildiği görülmektedir. Bir STİM'in sunduğu hizmetlerin devamlılığını ve kalitesini sağlamak için bu yaklaşımın gerçekçi ve doğru olduğu değerlendirilmektedir (AusCERT, 2011).

AusCERT siber olaylara karşı koyma hizmetini hem proaktif hem de reaktif bir hizmet olarak üyelerine sunmaktadır. Proaktif çalışma daha çok kaynaktan beslenmeyi, siber tehditleri farklı noktalardan takip edebilmeyi gerektiren bir süreçtir. AusCERT'in üyelerine sunduğu olaya karşı koyma hizmetleri proaktif çalışmalarının bir sonucu olarak görülmektedir. Proaktif çalışma ile bazen üye organizasyonların dahi farkına varamadıkları saldırıların tespit edilebildiği ve gerekli önlemlerin alındığı ifade edilmektedir (AusCERT, 2011).

Siber olaylara reaktif olarak karşı koymada AusCERT'e yapılan ihbarlar doğrultusunda hizmet sunulması söz konusudur. İhbarı yapan organizasyon siber olaya ilişkin olarak AusCERT'ten koordinasyon hizmeti veya olaya müdahale desteği hizmeti almak istediğini belirtmektedir. AusCERT tarafından üyelerine yerinde müdahale desteği sunulmamaktadır (AusCERT, 2011).

b. Tehditleri ve açıklıkları izleme ve değerlendirme

AusCERT tarafından sunulan ve güvenlik bültenleri ve erken uyarı sistemlerinden oluşan bir hizmettir. Bir koordinasyon merkezi olarak hizmet veren AusCERT, birçok kaynaktan küresel tehditleri ve açıklıkları izlemektedir. İzleme sürecinde elde edilen bilgilerin uzmanlar tarafından değerlendirilmesi sonucunda alınması gereken önlemlere ilişkin çeşitli öneriler hazırlanmakta ve üyelerin hizmetine sunulmaktadır (AusCERT, 2011).

c. Sertifika hizmetleri

AusCERT, Avustralya, Yeni Zelanda, Fiji ve Papua Yeni Gine'deki eğitim ve araştırma kuruluşlarına finansal olmayan işlemlerde kullanılmak üzere sınırsız sayıda güvenli yuva katmanı (Secure Sockets Layer - SSL) sertifikası sunmaktadır (AusCERT, 2011).

d. Eğitim

AusCERT, dünyadaki birçok STİM'e siber olayların yönetimine ilişkin birçok eğitim vermiştir. Yeni kurulan STİM'lere kurulum aşamasında ve STİM süreçleri konusunda destek hizmeti verilmektedir (AusCERT, 2011).

2.3.3 Hizmet verdiği kurum/kuruluşlar

AusCERT, Avustralya'daki kamu ve özel sektördeki bireysel ve kurumsal internet kullanıcılarına hizmet vermektedir. Avustralya kamu kurumları, sektörle ve teknoloji üreticileri ile yakın işbirliği içinde olan AusCERT, Avustralya, Yeni Zelanda ve Asya-Pasfik bölgesindeki müşterilerine siber olayların ele alınması konusunda öneriler sunmaktadır. Bütün Avustralya üniversitelerinin ve Yeni Zelanda'daki üniversitelerin çoğunluğunun AusCERT üyesi olduğu görülmektedir (APCERT, 2009).

2.3.4 Faaliyetleri

AusCERT, talep edilmesi halinde STİM eğitimlerini sunmaktadır. TERENA TF-STİM eğitimlerinden olan Transit'in Güney Kore'de FIRST'ün STİM eğitiminin ise Malezya'da verilmesini sağlamaktadır (APCERT, 2009).

Bunun dışında AusCERT tarafından her yıl Asya-Psifik bilgi güvenliği konferansı düzenlenmektedir. Söz konusu konferans 2009 yılında yaklaşık 1000 temsilcinin katılım ile Avustralya'da düzenlendiği ifade edilmektedir. Ayrıca ağ ve bilgi paylaşımı konulu çeşitli etkinlikler de yapılmaktadır (APCERT, 2009).

AusCERT uluslararası konferanslara da katılım sağlamaktadır. Çin'de düzenlenen APCERT 2009 konferansına, FIRST tarafından düzenlenen teknik konferansa ve ITU tarafından düzenlenen Asya-Pasifik siber güvenlik forumuna katılım sağladığı görülmektedir (APCERT, 2009).

2.4. Çin (CNCERT/CC)

Çin U-STİM/KM'si (China CERT/Coordination Centre - CNCERT/CC), ulusal kamu ağlarında meydana gelen güvenlik olayları konusunda Çin sınırları içerisindeki tüm STİM'ler arasında koordinasyonun sağlanmasından sorumlu ulusal bir STİM organizasyonudur. Ekim 2000'de kurulan CNCERT/CC Ağustos 2002'de FIRST'ün üyesi olmuştur. Yönetim kurulu üyesi olarak da APCERT'in kurulmasında aktif rol almıştır. Merkezi Pekin'de bulunan CNCERT/CC'nin 31 ilde şubesi bulunmaktadır (CNCERT/CC, 2008).

CNCERT/CC, Ulusal kamu ağlarında, önemli ulusal uygulama sistemlerinde meydana gelen güvenlik olaylarının ele alınmasına ilişkin tespit, tahmin, karşı koyma ve önleme çalışmalarını içeren ağ güvenliği hizmetleri sunmakta ve teknoloji desteği sağlamaktadır. İnternet güvenliği sorunlarına ilişkin bilgiler toplayan CNCERT/CC, bu bilgilerin doğruluğunu kontrol etmekte, onaylanan bilgileri yayımlamaktadır. Çin'in bilgi paylaşımından ve uluslararası organizasyonlarla koordinasyonundan sorumlu STİM olarak da hizmet vermektedir (CNCERT/CC, 2011).

2.4.1. Misyonu

CNCERT/CC'nin misyonu güvenli ulusal bir siber ortam sağlamak olarak ifade edilmektedir (CNCERT/CC, 2011).

2.4.2. Verdiği hizmetler

CNCERT/CC'nin yürüttüğü faaliyetler ve sunduğu hizmetler arasında bilgi toplama, olay izleme, siber olayları ele alma, verilerin analizi, siber olaylarla mücadelede kullanılacak kaynakları oluşturma, güvenlik araştırmaları yapma ve güvenlik eğitimleri verme, teknik danışmanlık yapma ve uluslararası STİM'lerle olan işlemleri yürütme yer almaktadır (CNCERT/CC, 2008).

Güvenlik olaylarını izleyen CNCERT/CC, tespit ettiği ciddi güvenlik problemlerine ilişkin ilgili organizasyonları tedbir almaları konusunda uyarmakta, bazen de alınan tedbirlerde teknik destek sağlayarak yardımcı olmaktadır (CNCERT/CC, 2008).

Her STİM'in sunması gereken en temel hizmet olan siber olayların ele alınması hizmeti de CNCERT/CC tarafından müşterilerine sunulmaktadır. CNCERT/CC, Çin sınırları içinden ve dünyanın herhangi bir yerinden yapılan siber tehdit veya siber olay ihbarlarını değerlendirmekte ve öncü birim olarak hareket etmektedir (CNCERT/CC, 2008).

STİM hizmetlerinin sunulması sürecinde kazanılan tecrübeler doğrultusunda elde edilen veriler kapsamlı bir analize tabi tutulmakta ve ilgili tüm tarafların güvenebileceği raporlar hazırlanmaktadır. Bunun yanı sıra açıklıklar, ürün yamaları, savunma araçları ve en son ağ güvenliği teknolojilerinden oluşan bir kaynak da CNCERT/CC tarafından oluşturulmaktadır (CNCERT/CC, 2008).

2.4.3. Hizmet verdiği kurum/kuruluşlar

CNCERT//CC, kamu kurumlarına, önemli ulusal uygulama sistemlerine ve kritik organizasyonlara siber olayların tespit edilmesi, öngörülmesi, siber olaylara karşı koyulması ve siber olaylardan korunması konularında ağ güvenlik hizmetleri sunmakta ve teknoloji desteği sağlamaktadır. İnternet güvenliğine ilişkin bilgiler CNCERT/CC tarafından toplanmakta, doğrulanmakta ve yayımlanmaktadır. Ayrıca Uluslararası güvenlik organizasyonları ile gerçekleştirilen bilgi paylaşımından ve koordinasyondan da CNCERT/CC sorumludur (CNCERT/CC, 2008).

2.4.4. Faaliyetleri

2008 yılında iç ve dış kullanıcılardan ve kurumlardan CNCERT/CC'ye 5.167 siber güvenlik olayının raporlandığı görülmektedir. Olay raporlarının büyük çoğunluğunun (1.849) istem dışı elektronik postaya ilişkin olduğu, yemlemeye ilişkin 1.256, kötücül kodlara ilişkin ise 1.227 ihbarın yapıldığı ifade edilmektedir. Bir önceki yıla oranla istem dışı elektronik posta ihbar sayısının %54.5, kötücül kod ihbar sayısının ise %6.6 artış gösterdiği, yemleme ihbar sayısının %5.3 azaldığı bilgisine yer verilmektedir (CNCERT/CC, 2008).

2008 yılında ele alınan siber olay sayısına bakıldığında internet sayfasının bozulması, yemleme, internet sayfalarına yerleştirilmiş kötücül kod, DoS ve kötücül yazılımları kapsayan 1.173 olaya müdahale edildiği görülmektedir (CNCERT/CC, 2008).

CNCERT/CC tarafından yapılan trafik analizlerinde İletim Kontrol Protokolü (Transmission Control Protocol - TCP) trafiğinin ilk 5 uygulamasının http, P2P ve elektronik posta uygulamaları olduğu görülmektedir (Tablo 2.3).

Tablo 2.3. CNCERT/CC - 2008 yılında TCP trafiğindeki ilk 10 uygulama

TCP Portu	Sıra	Yüzde (%)	Uygulama
80	1	28.36	http
8080	2	1.00	http
4662	3	0.93	eMule
443	4	0.80	HTTPS
25	5	0.60	SMTP

Kaynak: (CNCERT/CC, 2008)

Yine 2008 yılında kullanıcı datagram protokolü (User Datagram Protocol - UDP) trafiğndeki ilk 3 uygulama Xunlei[3], QQ ve QQ IM[4] şeklinde sıralanmaktadır (Tablo 2.4).

Tablo 2.4. CNCERT/CC - 2008 yılında UDP trafiğindeki ilk 10 uygulama

UDP Portu	Sıra	Yüzde (%)	Uygulama
15000	1	3.70	Xunlei
29909	2	1.02	QQ
8000	3	0.94	QQ IM
80	4	0.84	http
53	5	0.74	DNS

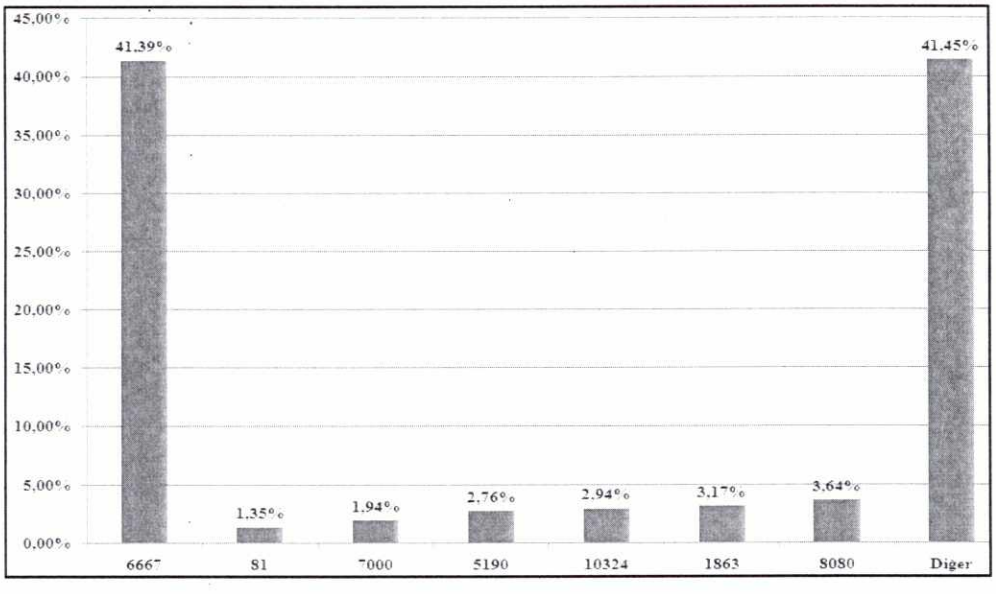
Kaynak: (CNCERT/CC, 2008)

[3] İnternetten dosya indiren bir yazılım

[4] QQ ve QQ IM Çin'de yaygın bir şekilde kullanılan programın sohbet ve dosya indirme sürümleri

Bazı popüler solucanlarla ilgili yapılan izleme çalışmaları sonucunda Çin'deki trojanların içine yerleştirilmiş 565.605 adet IP adresi tespit edilmiştir. Bu IP adreslerinin düzenlenecek herhangi bir saldırının kaynağı veya elde edilen bilgilerin gönderileceği hedef sistemin adresi olarak kullanılabileceği düşünülmektedir. 2008 yılındaki bu rakamın 2007 yılına göre % 43,2 azaldığı ifade edilmektedir. Bunun yanı sıra yine 2008 yılında Çin'deki 1.237.043 bilgisayar köle bilgisayar yazılımının yerleştirildiği tespit edilmiştir. Ayrıca Çin'deki köle bilgisayarları Çin sınırları dışından kontrol eden 5.210 adet KBA kontrol sunucusu tespit edilmiştir. Bu sunucuların %31'inin ABD'de, %10'unun Macaristan'da ve %5'inin Güney Kore'de olduğu ifade edilmektedir. KB'lar tarafından kullanılan portlara bakıldığında ise (Şekil 2.4) ilk 3 sırada %41.39 ile 6667[5] numaralı portun, % 3.64 ile 8080 numaralı portun, % 3.17 ile ise 1863[6] numaralı portun geldiği görülmektedir.

Şekil 2.4. IRC KBA'ları ve kontrol sunucuları tarafından kullanılan portlar



Kaynak: CNCERT/CC, 2008

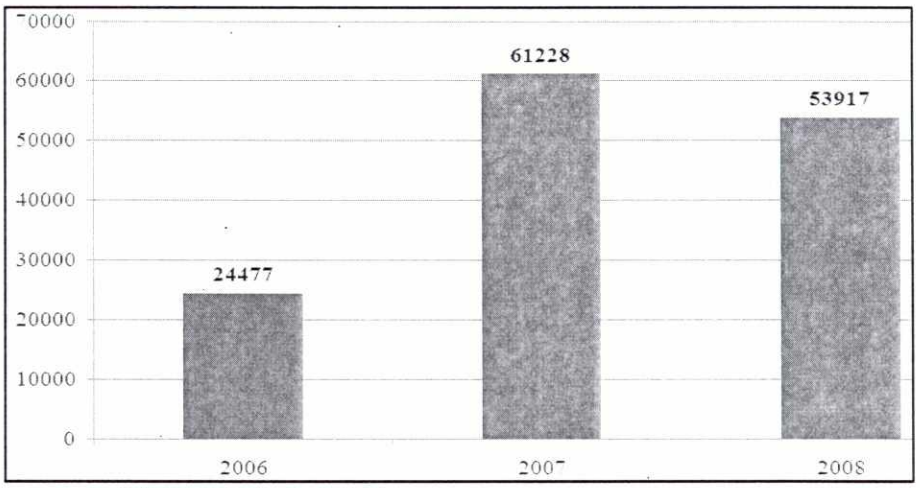
2008 yılında Çin'de hizmet veren 53.917 adet internet sayfasının gerçekleşen saldırılar sonucunda hizmetinin aksadığı tespit edilmiştir (Şekil 2.5). Elde edilen verilere bakıldığında alınan güvenlik önlemlerinin yetersiz ve zayıf olmasından

[5] 6667 numaralı port sohbet kanalı (Internet Relay Chat - IRC) tarafından kullanılmaktadır.

[6] 1863 numaralı port Microsoft sohbet uygulaması MSN tarafından kullanılmaktadır.

dolayı kamu kurumlarının internet sayfalarına saldırılmasının daha kolay olduğu sonucu çıkarılmıştır.

Şekil 2.5. 2006–2008 arasında siber saldırı ile bozulan internet sayfaları



Kaynak: (CNCERT/CC, 2008)

CNCERT/CC'nin katılım sağladığı bölgesel faaliyetler arasında Kasım 2008'de APCERT tarafından gerçekleştirilen siber olayların ele alınması tatbikatı yer almaktadır (CNCERT/CC, 2011).

CNCERT/CC'nin siber tehditlerin önlenmesi, azaltılması ve bu tehditlere müdahale edilmesi amacıyla dünyanın dört bir yanındaki STİM birlikleri ile gerçekleştirdiği işbirliklerinden sağlanan desteğin çok önemli olduğu görülmektedir.

2.5. Dünya Uygulamalarına İlişkin Değerlendirme

STİM dünya uygulamalarına bakıldığında hemen her ülkenin bir U-STİM'e veya Kamu-STİM'e sahip olduğu görülmektedir. Sadece U-STİM'in olduğu durumlarda bu yapının Kamu-STİM gibi de faaliyet gösterdiği görülmektedir. Aynı şey tersi durumda da söz konusu olmaktadır. Avustralya gibi bazı ülkelerde ise hem U-STİM hem de Kamu-STİM hizmet bulunmaktadır.

Misyonlarına bakıldığında hemen her U-STİM'in hedefinin ülkeleri için güvenli ve güvenilir bir siber ortam oluşturmak olduğu görülmektedir. Bu misyonu gerçekleştirmek amacıyla her sektörden müşteriye hizmet verilmesi de STİM'lerin ortak yanları arasında yer almaktadır.

STİM'lerin yapılanmalarına bakıldığında hem kamu, hem özel hem de kamu-özel işbirliği şeklinde yapılanmalar görülmektedir. Bir kamu-özel yapılanması olan US-CERT Carnegie Mellon Üniversitesi bünyesinde kurulan CERT/CC ile yakın işbirliği içinde çalışmaktadır. Benzeri bir işbirliği AusCERT ile yine Avustralya'daki Queensland Üniversitesi arasında da bulunmaktadır. STİM alanında araştırmalar yapılması, siber tehditlere müdahalede kullanılacak araçların ve çözüm önerilerinin geliştirilmesi bağlamında bir U-STİM'in bir üniversite ile işbirliği kurması önem arz etmektedir.

STİM yapılarının genellikle merkezi olması, personel sayılarının çok fazla olmaması müşterilere operasyonel destek sağlanmasını zorlaştıran nedenler arasında yer almaktadır. Bundan dolayı U-STİM'ler müşterilerine genellikle olay koordinasyon hizmeti vermektedir. AusCERT'in ise müşterilerinin talep etmesi durumunda olaya yerinde müdahale desteği de verdiği görülmektedir.

STİM'ler çoğunlukla üyelerinden topladıkları aidatlarla kendilerini finanse etmektedirler. Müşterisi kamu kurumları olan STİM'lerin ise devlet tarafından ya doğrudan ya da proje desteği şeklinde fonlandığı görülmektedir.

U-STİM'lerin genelde bir bakanlığın koordinasyonunda ya da kamu temsilcisinin yönetim kurulunda yer alması şeklinde yapılandığı görülmektedir. Örneğin Hollanda'da İçişleri ve Kraliyet Bakanlığı GOVCERT.NL'nin komisyon üyesidir.

Her STİM, en az bir uluslararası platforma üye olmakta ve bu platformda aktif bir şekilde görev almaktadır. Bu bilgi paylaşımı ve işbirliği tecrübesi hizmet için oluşturulan araçlara da yansımaktadır. FIRST'ün ve EGC'nin aktif ve başarılı bir üyesi olan GOVCERT.NL, olaylara müdahale de Taranis gibi etkin bir iş akış modeli ve aracı geliştirmiştir.

Bazı STİM'lerin kendi ülkeleri dışından müşterilere hizmet vermesi de söz konusu olabilmektedir. Örneğin AusCERT Avustralya dışında Yeni Zelanda ve Asya-Pasfik bölgesindeki müşterilerine de güvenlik önerileri sunmaktadır.

Çin büyük bir coğrafyaya sahip olmasından dolayı CNCERT/CC'nin 31 şube şeklinde yapılandırıldığı görülmektedir. Bu dağıtık yapılanma ile olaylara yerinde müdahale imkânı ortaya çıkmış olmaktadır.

3. ULUSLARARASI İŞBİRLİĞİ PLATFORMLARI

Sınır aşan bir yapıya sahip olan siber tehditlerle ve siber olaylarla mücadelede başarı uluslararası işbirliğine bağlanmaktadır. Zira bir siber olayı gerçekleştiren suçlular farklı ülkelerde, olayın hedefi olan organizasyon veya sistemler başka bir coğrafyada ve olayı kontrol eden sunucular çok daha farklı bir noktada bulunabilmektedir. Böyle bir durumda uluslararası işbirliği olmaksızın siber olayın başarılı bir şekilde bertaraf edilmesi ve olayı gerçekleştirenlerin belirlenmesi mümkün olmamaktadır.

Siber ortamda U-STİM'ler ve STİM'ler ile uluslararası işbirliği, kurulan çeşitli platformlar aracılığıyla gerçekleşmektedir. Bu platformlar arasında ITU'nun bünyesinde kurulan ve ITU'ya üye ülkelerin yararlanabildikleri siber tehditlere karşı uluslararası çok taraflı ortaklık (International Multilateral Partnership Against Cyber Threats - IMPACT), hemen her sektörden STİM üyesine sahip FIRST ve Avrupa Ağ ve Bilgi Güvenliği Ajansı'na (European Network and Information Security Agency - ENISA) yer almaktadır.

3.1. ITU-IMPACT

Devletler, ulusal siber güvenlik çalışmalarına tüm tarafları kapsayacak şekilde öncülük edebilecek konumda görülmektedir. Siber tehditlerle mücadelede alınması gereken asıl önlemler dışında devletlerin, tüm taraflar arasında siber güvenliğin anlaşılmasını, farkındalığın artmasını ve tarafların rolünün ve sorumluluğunun belirlenmesini sağlamak gibi önemli bir görevinin olması gerektiği belirtilmektedir (ITU, 2009).

ITU'nun Küresel Siber Güvenlik Ajandası (Global Cybersecurity Agenda- GCA) ve yine ITU'nun kritik bilgi altyapılarının korunması çalışması çerçevesinde, devletlerin siber güvenlik konusunda üstlenebilecekleri roller aşağıdaki şekilde sıralanmaktadır (ITU, 2009):

- Politika yapmak (ulusal bir siber güvenlik stratejisi oluşturmak),
- Hukuki önlemler almak,
- Kurumsal yapılar oluşturmak,

- Kurumsal yapılar kurmak ve koordinasyonu sağlamak ve
- Siber olayların yönetimini sağlamak ve siber güvenlik hazırlık değerlendirmesi yapmak.

- Ulusal siber güvenlik kapasitesini geliştirmek,
- Kamu-özel sektör arasındaki işbirliğini sağlamak ve elektronik haberleşme sektörünü düzenlemek.

Siber tehditlerin tespit edilmesi, soruşturulması, analiz edilmesi ve bu tehditlere karşı koyulması amacıyla ulusal ve uluslararası düzeyde çeşitli STİM'ler kurulmuştur. Söz konusu STİM'ler, sundukları hizmetler ve hizmet sundukları müşteriler bakımından farklılıklar göstermektedir (ITU, 2009).

Her ne kadar farklı alanlarda farklı STİM'ler kurulmuş olsa da ülke için ulusal düzeyde etkin bir şekilde faaliyette bulunacak bir STİM'in kurulmasının zorunlu olduğu kabul edilmektedir. Zira siber güvenliğe hazırlık çalışmalarında ve büyük ölçekli siber saldırılara karşı koyulmasında ulusal STİM'in doğal olarak sorumluluk alması söz konusudur (ITU, 2009). STİM'lerin uluslararası işbirliği platformlarında yer almalarının bir gereklilik olduğunu söylemek de mümkündür.

Söz konusu uluslararası platformlardan biri olan IMPACT, Birleşmiş Milletlerin (BM) uzman ajansı ITU'nun kar amacı gütmeyen ve kapsamlı bir kamu-özel sektör işbirliğiyle kurulmuş siber güvenlik yürütme kolu olarak tanımlanmaktadır. Merkezi Malezya'da olan IMPACT, devlet, akademi ve elektronik haberleşme sektöründen uzmanları bir araya getirerek siber tehditler konusundaki küresel yetenekleri arttırmayı amaçlamaktadır. Siber tehditlerle mücadelede kullanılmak üzere, ITU'ya üye 192 ülkenin IMPACT bünyesindeki kaynaklara erişme imkânı bulunmaktadır (IMPACT, 2011).

Siber tehditlerin hızlı bir şekilde artması ve yaygınlaşması, ülkelerin ekonomik ve sosyal hayatlarını önemli oranda risk altına sokmaktadır. Ülkelerin bu tehditler ve risklerle sadece kendi önlemleri ve kaynakları ile mücadele etmeleri mümkün olmamaktadır. Birçok durumda siber tehditlerle veya siber olaylarla mücadeleye ilişkin çözümlerin akademik çevrelerden veya özel sektörden çıktığına vurgu

yapılmaktadır. Dolayısıyla siber âlemin güvenliğinin sağlanması için mümkün olan tüm tarafların bir araya gelerek çözüme ilişkin bilgileri ve kaynakları paylaşmaları gerekmektedir. Uzman ekipler arasında işbirlikleri kurulmadan ve bilgi paylaşımı olmadan ülkelerin tek başına siber tehditlerle mücadele edebilecek yetenek seviyesini yakalama imkânı bulunmamaktadır. IMPACT'in bu boşluğu doldurma amacında olduğu ifade edilmektedir (IMPACT, 2011).

IMPACT'in bünyesinde küresel müdahale merkezi (Global Response Center - GRC), politika ve uluslararası işbirliği merkezi, eğitim ve beceri geliştirme merkezi ve güvenlik güvence ve araştırma merkezi bulunmaktadır (IMPACT, 2011).

3.1.1 GRC

GRC'nin siber tehditlerle mücadele konusunda dünyanın önde gelen merkezi olma amacında olduğu ifade edilmektedir. Akademik dünyadan, ülkelerden ve elektronik haberleşme sektöründen lider birçok ortakla çalışmanın neticesi olarak GRC, gerçeğe yakın bir erken uyarı sistemi sunmaktadır. IMPACT'in merkezi olarak tanımlanan GRC'de, bir kriz odası, en yeni bilgi teknolojisi ürünleri ve haberleşme araçları, sürekli çalışan ve tam işlevsel bir güvenlik operasyon merkezi, çok iyi korunan güvenli bir veri merkezi ve vardiyalı çalışan personel için imkânlar bulunmaktadır (IMPACT, 2011).

GRC kendi içerisinde ağ erken uyarı sistemi (Network Early Warning System - NEWS) ve uzmanlar için elektronik güvenli işbirliği platformu (Electronically Secure Collaborative Application Platform for Experts - ESCAPE) olmak üzere iki ayrı platformdan oluşmaktadır. IMPACT üyelerine NEWS ve ESCAPE platformlarına erişme imkânı sunulmaktadır (IMPACT, 2011).

GRC'nin sağladığı temel özellikler arasında: NEWS, uzman bulucu, takım yönetimi, onarım imkânı, otomatik tehdit analiz sistemi, eğilim kaynakları, tehditlerin küresel görünümü, ülkeye özel siber tehditler, siber olay yönetimi, eğilim izleme ve analiz, bilgi bankası, raporlama ve bal küpü ağı sayılmaktadır (IMPACT, 2011).

a. ESCAPE

ESCAPE, farklı ülkelerden siber güvenlik konusunda uzman yetkili kişilerin güvenli bir şekilde işbirliği kurabildikleri, bilgi paylaşımında bulundukları elektronik bir ortamdır. Bu sayede üye ülkelerin özellikle de kriz sırasında siber tehditlere anında karşı koyabilme olanağı sağlandığı değerlendirilmektedir. ESCAPE, acil durumlarda üye ülkelerin hızlı bir şekilde bilgi ve kaynak paylaşımında bulunmalarını sağlayarak GRC'ye tek koordinasyon ve karşı koyma merkezi olma özelliği kazandırmaktadır (IMPACT, 2011).

b. NEWS

NEWS, farklı erken uyarı sistemlerinden ve siber güvenlik ürün üreticilerinden derlenen bilgilerden oluşan bir sistem olarak hizmet vermektedir. NEWS'in amacı, doğru bilginin ilgili birimlere zamanında ulaştırılarak dünyanın herhangi bir yerinden kaynaklanan siber tehditlere etkin bir şekilde müdahale edilmesini sağlamaktır (IMPACT, 2011).

Siber güvenlik alanında faaliyet gösteren ve IMPACT ile işbirliği içinde çalışan firmalardan siber tehditlere ilişkin çok miktarda bilgi paylaşılmakta ve bu bilgiler NEWS üzerinden üyelere dağıtılmaktadır. NEWS'in siber tehditler konusunda en zengin bilgi bankası olması amaçlanmaktadır (IMPACT, 2011).

3.1.2 Politika ve uluslararası işbirliği merkezi

Siber âlemin modern toplumların hayatlarını hemen her yönüyle etkilediği bilinmektedir. Bunun yanı sıra siber âlemin ekonomi, sivil altyapılar, kamu güvenliği ve ulusal güvenlik açısından önemi son derece kritiktir. Dünya üzerindeki yüzlerce ülkeyi, milyarlarca insanı birbirine bağlayan bir ortam olarak internet, yaşam tarzlarını ve ilişkileri hayal dahi edilemeyecek bir şekilde dönüştürmüş ve değiştirmiştir (IMPACT, 2011).

İnternet ortamına erişimin kolay olması, göreceli anonimlik sağlaması ve sınırları aşması siber tehditlerin de artmasına ve ülkeleri, iş dünyasını ve bireyleri tehdit eden bir tehlike haline gelmesine yol açmaktadır. IMPACT, uluslararası bir sorun olarak değerlendirilen siber tehdit probleminin kapsamına, şiddetine ve yapısına ilişkin etkin çalışmaların yapılması gerektiğine inanmaktadır. Siber ortamda düzenin ve istikrarın sağlanması, güvenin tesis edilmesi ve internetin kötüye kullanımının engellenmesi için yeni politikaların, düzenlemelerin ve yeni yapıların oluşturulması gerekmektedir. Oluşturulan politikaların ulusal sınırlar içerisinde uygulanabilir olmasına dikkat edilmesi büyük önem arz etmektedir (IMPACT, 2011).

Siber âlemin hem ulusal hem de uluslararası bağlamda yönetilmesi zor bir hal aldığı, siber tehditlerle mücadelede tehditlerin hedefi olabilecek tüm tarafların bir araya gelerek işbirliği içinde çalışmalarına, politikalar üretmelerine ihtiyaç duyulduğu ifade edilmektedir. IMPACT bünyesinde kurulan politika ve uluslararası işbirliği merkezinin bu ihtiyacı giderme amacında olduğunu söylemek mümkündür (IMPACT, 2011).

Politika merkezi mevcut durumda:

- Siber kanunların desteklenmesi ve ulusal siber suç mevzuatlarının küresel olarak uyumlaştırılması,
- Farkındalığın arttırılması ve siber suçların ve siber tehditlerin azaltılması,
- Çocukların internette korunmasına ilişkin sorunlar ve çözümlerin desteklenmesi

konularında çalışmaktadır (IMPACT, 2011).

Merkez, farkındalığı arttırmak ve uluslararası işbirliğini teşvik etmek üzere çeşitli faaliyetlere katılmaktadır. Söz konusu faaliyetlerden biri de IMPACT tarafından yıllık olarak düzenlenen dünya siber güvenlik zirvesidir (World Cyber Security Summit - WCSS) (IMPACT, 2011).

Uluslararası işbirliği merkezi, hükümetleri, elektronik haberleşme sektörünü, akademik çevreleri, düşünce kuruluşlarını, özel ilgi gruplarını ve BM, ITU, Interpol

ve Avrupa Konseyi (AK) gibi uluslararası organizasyonları işbirliği amacıyla bir araya getiren IMPACT'in temas noktası olarak hizmet vermektedir. IMPACT işbirliği platformunun ITU'ya üye 192 ülke ile de işbirliği kurma imkânları sunduğu ifade edilmektedir (IMPACT, 2011).

3.1.3 Eğitim ve beceri geliştirme merkezi

Eğitim ve beceri geliştirme merkezinin siber güvenlik konusunda dünya çapında bir eğitim verdiği ifade edilmektedir. Verilen tüm eğitimler, seminerlerin ITU, Uluslararası Elektronik Ticaret Danışmanları Konseyi (The International Council of Electronic Commerce Consultants - EC-Council) ve SANS enstitüsü gibi önde gelen organizasyonlar ve bilgi teknolojisi firmaları ile işbirliği içinde verilmektedir (IMPACT, 2011).

Düzenlenen özel kurslar, siber tehditlere müdahale konusunda sahip olunan yeteneklerin arttırılması amacıyla küresel uzmanları bir araya getirmeyi, IMPACT'e hükümetlerle ve organizasyonlarla birlikte çalışma imkânı sağlamaktadır (IMPACT, 2011).

3.1.4 Güvenlik güvence ve araştırma merkezi

İleri teknoloji ile birbirine bağlı bir dünyada kamunun detaylı bir siber güvenlik programına ihtiyaç duyduğu görülmektedir. Güvenlik programı oluşturmanın en önemli parametresi bir güvenlik politikasının oluşturulması ve uygulanmasıdır. Bunu sağlamak ve siber güvenliğin mevcut durumunun anlaşılmasına yardımcı olmak çok ciddi bir çalışma sürecini gerektirmektedir. Aslında her hükümetin bir siber güvenlik politikası olmasına karşın, politikaların uygulanmasının genellikle zor olduğu gerçeği dile getirilmektedir. Uygulama ile uygum sağlanması açısından IMPACT Devlet Güvenlik Puan Kartı (IMPACT Government Security Scorecard - IGSS) gibi bir çözüme ihtiyaç duyulduğuna inanılmaktadır (IMPACT, 2011).

Hükümetin kritik uygulamalarının ve altyapılarının merkezi ve otomatik bir şekilde analiz edilmesi sayesinde, zayıflıkların tespit edilmesi ve gerekli önlemlerin alınması

imkânı doğmaktadır. Buna ilave olarak risklerin yetkili personel tarafından etkin bir şekilde yönetilmesi de söz konusu olabilmektedir. IGSS'nin hükümetin mevcut güvenlik durumunu görmesini sağladığı, alınması gereken önlemler konusunda fikirler verdiği ifade edilmektedir (IMPACT, 2011).

IGSS'nin en temel özellikleri arasında:

- Aracısız bir mimaride olması,
- Platform bağımsız olması ve bütün platform ve teknolojilerle çalışması,
- Tüm önemli standartlara sahip olması (Uluslararası Standardizasyon Örgütü (International Organization For Standardization - ISO) 27001 bilgi güvenliği yönetim sistemi, ISO 25999 iş sürekliliği gibi),
- Güçlü raporlama kapasitesine sahip olması

sayılmaktadır (IMPACT, 2011).

STİM dünyasının gelişimine katkıda bulunmak için bilginin ve teknolojinin politikadan ve ticari kaygılardan uzak bir platformda toplanmasına ihtiyaç olduğu değerlendirilmektedir. Aslında bu fikrin hemen her STİM işbirliği platformları tarafından dile getirilen bir ihtiyaç olduğunu söylemek mümkündür. IMPACT bünyesinde bulunan CIRT-LITE platformu sayesinde, özellikle de gelişmekte olan egemen ulusların siber güvenlik alanındaki kendilerine özgü sorunlarına cevap olabilecek politikalar geliştirebilecekleri ve uygulayabilecekleri ifade edilmektedir. CIRT-LITE platformu ile çok sayıda şablon politika dokümanı ülkelerin kullanımına sunulmaktadır. Söz konusu dokümanlar, roller ve sorumluluklar, iş akışları, ekipman kullanımı, sayısal delillerin tespiti, toplanması ve saklanması gibi konu başlıklarında değişiklikler yapılmak suretiyle kullanılabilmektedir (IMPACT, 2011).

Araştırma merkezinde akademi ve araştırma topluluklarından bir araya gelen uzmanlar siber güvenlik alanında karşılaşılan sorunları analiz etmekte ve bu sorunlara çözümler üretmektedirler. Araştırma merkezinde gelecekte çığır açacak üç önemli alandaki çalışmalar koordine edilmektedir (IMPACT, 2011):

- Veri madenciliği ve tehdit araştırması,

- Köle bilgisayar araştırması ve
- IMPACT Çevrimiçi araştırma ağı (IMPACT Research Online Network - IRON).

Araştırma merkezi bünyesindeki özel bilgi teknolojisi laboratuarları ve özel ekipmanlar gibi ileri araştırma imkânları, merkeze üye olan STİM'lerin hizmetine sunulmaktadır (IMPACT, 2011).

Araştırma merkezi, siber güvenlik alanında doğrudan üniversitelerle ve yükseköğrenim kurumları ile işbirliği yapmaktadır. Mevcut durumda işbirliği kurulan akademik kurumlarla:

- Bilgi paylaşımı ve değişimi,
- Ortak öğretim programlarının geliştirilmesi,
- Onaylanmış eğitim kurslarının verilmesi,
- Ortak araştırma faaliyetlerinin ve yayınlarının geliştirilmesi,
- Araştırmaların desteklenmesi için olası fırsatlar ve
- IRON

gibi konularda çalışmalar yapılmaktadır (IMPACT, 2011).

IMPACT araştırma merkezinin, özel sektör, akademik çevreler ve uluslararası sertifika kuruluşları ile işbirliği ortaklığı bulunmaktadır. Sektörden Microsoft, Kaspersky, Symantec, F-Secure, Trend Micro gibi firmalarla işbirliği ortaklıkları yapılmıştır. Uluslararası sertifika kuruluşları arasından, SANS, Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu (Information Systems Security Certification Consortium, Inc. – $(ISC)^2$) ve EC-Council, üniversiteler arasından ise Bonn üniversitesi, Afrika üniversiteler birliği ve Malezya Utara üniversitesi ile işbirliği yapılmaktadır (IMPACT, 2011).

Bunların yanı sıra uluslararası örgütlerle de işbirliği örnekleri bulunmaktadır. Bunlar arasında İngiliz Uluslar Örgütü Telekomünikasyon Birliği (Commonwealth Telecommunications Organisation - CTO) gelmektedir (IMPACT, 2011).

3.2. AB-ENISA

AK, gelişen dijital ekonomi için 2020 yılını hedef alan Avrupa Dijital Ajandası (ADA) adı ile bir strateji oluşturmuştur. Söz konusu strateji, yaşanan dijital devrimden en fazla faydayı elde etmeyi amaçlayan politikalar ve eylemleri konu edinmektedir. Stratejide belirlenen hedeflerin gerçekleştirilmesi amacıyla AK'nin ulusal hükümetlerle yakın işbirliği içinde çalışması, kaydedilen ilerlemelerin ve karşılaşılan sorunların değerlendirileceği yıllık toplantıların yapılması hedeflenmektedir (EC, 2010).

Söz konusu stratejinin "Güven ve Güvenlik" başlıklı bölümünde atılması planlanan adımlar arasında, bilgi sistemlerini hedef alan siber tehditlerle mücadele edilmesi ve AB üyesi ülkelerin U-STİM kurmaları yer almaktadır (EC, 2010).

ADA'nın 29 uncu eylemi: Bilgi sistemlerini hedef alan siber tehditlerle mücadele edilmesi

Bilgi sistemlerini hedef alan siber tehdit sayısının giderek artması probleminden yola çıkılarak hazırlanan 29 uncu eylemle, bilgi sistemlerini hedef alan siber tehditlerle mücadele edilmesi için; 2010 yılı sonu itibariyle yasal girişimler de dâhil olmak üzere önlemler sunulması, 2013 sonu itibariyle ise Avrupa'da ve uluslararası düzeyde siber yargıya ilişkin kuralların koyulması hedeflenmektedir. AB'nin bu konuda harekete geçmesi, AB kolluk kuvvetlerini siber suçlarla mücadele etmeleri için gelişmiş araçlarla donatmayı amaçlamasından kaynaklanmaktadır (EC, 2010).

29 numaralı eylem kapsamında 2011 yılında, bilgi sistemlerini hedef alan saldırılar hakkındaki taslak AB Direktifinin kabul edilmesi çalışmalarının devam edeceği belirtilmektedir. 2012 yılında ise söz konusu direktif müzakerelerinin sonlandırılması ve tüm AB düzeyinde kabul edilmesinin sağlanması hedeflenmektedir. Üye ülkelerin söz konusu direktifin kabul edilmesinden sonra iki yıl içerisinde gerekli önlemeleri almaları gerekmektedir (EC, 2010).

ADA'nın 38 inci eylemi: AB üyesi ülkelerin U-STİM kurmaları

38 numaralı eylem kapsamında, tüm üye ülkelerin 2012 yılına kadar iyi bir şekilde işleyen U-STİM kurmaları gerekmektedir. Üye ülkelerin U-STİM kurmaları ihtiyacı, siber saldırılara karşı gösterilen tepkilerin çok yavaş olduğu tespitinden yola çıkılarak ortaya koyulmuştur. Çevrimiçi siber olaylara zamanında müdahale edilebilmesi için Avrupa'da iyi işleyen bir STİM ağının oluşturulması gerektiği belirtilmektedir. AB, siber tehditlere AB çapında daha hızlı tepki verme kapasitesinin güçlendirilmesi amacıyla üye ülkelerin U-STİM kurmaları konusunda harekete geçmiştir. Ayrıca AK, hali hazırda var olan U-STİM'ler arasındaki işbirliğinin güçlendirilmesi konusunda üye ülkelere çağrıda bulunmaktadır. (EC, 2010).

AB üyesi ülkelerde U-STİM yapısının kurulması ile:

- Siber saldırılardan etkilenenlere acil müdahale hizmeti sunulması
- Çevrimiçi tehditlere ilişkin uyarıların yayımlanması ve
- Ağ güvenliğinin geliştirilmesine katkı sağlayacak diğer bilgilerin sunulması

hizmetlerinin verilmesi imkânının oluştuğu belirtilmektedir (EC, 2010).

ADA'nın 38 inci Eylemi ile 2011 yılında AB üyesi tüm ülkelerde iyi işleyen U-STİM veya Kamu-STİM yapılarının kurulması, söz konusu STİM'ler arasındaki işbirliğinin güçlendirilmesi konusunda ENISA'nın destek çalışmalarının yürütülmesi planlanmaktadır. 2012 yılında ise U-STİM veya Kamu-STİM'lerden oluşan ağın kurulumunun tamamlanması hedeflenmektedir (EC, 2010).

ENISA, ağ ve bilgi sistemlerinde meydana gelen problemleri önlemek, belirlemek ve bu problemlere karşı koymak üzere Avrupa Birliği'nin (AB), AB'ye üye ülkelerin ve iş dünyasının kapasitesini arttırmak amacıyla kurulmuştur. Bu hedeflerin gerçekleştirilmesi için ENISA, bir ağ ve bilgi güvenliği uzmanlık merkezi olarak çalışmakta ve kamu ve özel sektör arasında işbirliği kurulmasını teşvik etmektedir (ENISA, 2011).

Ağ ve bilgi güvenliği problemlerine müdahale edilmesinde, bu problemlerin tespit edilmesinde ve özellikle de önlenmesinde ENISA Avrupa Komisyonu'na, üye ülkelere ve iş dünyasına yardımcı olmaktadır (ENISA, 2011).

Bir uzmanlık merkezi olan ENISA, bilgi güvenliği alanındaki çok özel teknik ve bilimsel görevleri yapmak üzere AB tarafından kurulmuştur. AB'nin ağ ve bilgi güvenliği alanındaki mevzuatının güncelleme çalışmalarında da ENISA destek vermektedir (ENISA, 2011).

3.2.1 Misyonu

İletişim ağlarının ve bilgi sistemlerinin ekonomik ve toplumsal hayatta önemli bir faktör olduğu gerçeğinden hareketle, güvenli ağların sayısal ekonomiler için su ve elektrik desteği kadar hayati öneme sahip olduğu ifade edilmektedir. Bunun sonucu olarak iletişim ağlarının ve bilgi sistemlerinin güvenliğinin toplumda artan bir endişe kaynağı olmaktadır. Bu endişenin bilgi sistemlerinin karmaşıklığından, bu sistemlerde meydana gelen kazalardan ve hatalardan ve bu sistemleri hedef alan siber saldırılardan kaynaklandığını ifade edilmektedir (ENISA, 2011).

Etkin ve güvenli bir şekilde işleyen ağların başta vatandaşların bilgi sistemlerine ilişkin yaşadıkları endişenin giderilmesi olmak üzere, pazarın düzgün bir şekilde işleyişine ve vatandaşların günlük yaşamlarına somut olarak katkısının olduğundan hareketle ENISA'nın, AB içinde yüksek ve etkin bir ağ ve bilgi güvenliği seviyesini yakalama ve ilgili paydaşlarla birlikte bir bilgi güvenliği kültürü oluşturma misyonu bulunmaktadır (ENISA, 2011).

3.2.2 Görev ve faaliyetleri

ENISA'nın düzenleme alanındaki temel görevleri arasında:

- Bilgi güvenliği konusunda ve sektörle olan ilişkilerinde donanım ve yazılım ürünlerindeki güvenlik sorunlarının belirlenmesinde AB'ye ve üye ülkelere danışmanlık ve destek sağlamak,

- Avrupa'da meydana gelen siber olaylara ve artan risklere ilişkin verileri toplamak ve analiz etmek,
- Bilgi güvenliği tehditleri ile başa çıkmak için yetenekleri geliştirmek üzere risk değerlendirmesi ve risk yönetim metotları geliştirmek,
- Farkındalığı arttırmak ve farklı taraflar arasında işbirliği geliştirmek

sayılmaktadır (ENISA, 2011).

3.2.3 Mevzuatı

Tüm AB faaliyetlerinde olduğu gibi bilgi güvenliği konusunda da yapılabileceklerin temelini oluşturmaktadır. ENISA'nın temel mevzuatı 460/2004 sayılı kuruluş mevzuatı olarak ifade edilmektedir (ENISA, 2011).

3.2.4 STİM alanındaki çalışmaları

Estonya'ya düzenlenen siber saldırı, Almanya'da, İsveç'te, Fransa'da ve diğer ülkelerde hükümetleri hedef alan siber saldırılar STİM'e olan ilginin artmasına yol açmıştır. Avrupa'daki çeşitli gruplar siber olaylarla mücadele için işbirliğinin gerekli olduğu sonucuna varmışlardır. Zira internetteki saldırıların geleneksel ülke sınırlarını aşan yapısı bu sonuca ulaşmadaki en önemli etken olarak görülmektedir. 1990'lı yılların başlarında bu tür işbirliğinin TERENA TF-CSIRT ve EGC grubu gibi birlikler arasında gerçekleştiği görülmektedir. Zamanla büyüyen bu birlikler ağ ve bilgi güvenliği için zengin bilgi, araç ve faaliyetler kaynağı olarak dile getirilmektedir (ENISA, 2011).

ENISA ağ ve bilgi güvenliği alanında operasyonel bir rol üstlenmemektedir. Bundan daha ziyade işleri kolaylaştırıcı ve bilgi kaynağı bir merkez olarak hizmet vermektedir (ENISA, 2011).

Büyük İSS'lerin kötüye kullanıma karşı oluşturdukları ekipler istenmeyen elektronik posta ve kötüye kullanım ile mücadele etmektedir. Benzer şekilde yazılım firmaları ürünleri ile ilgili güvenlik bilgilerini müşterilerinin kullanımına sunmaktadır. Son olarak da toplum destekli WARPs'ların güvenlik konusundaki bilgileri paylaşarak

üyelerine yardımcı oldukları görülmektedir. STİM konusunda çalışmalar yapan ENISA, kendi kullanıcılarına güvenlik hizmeti veren söz konusu grupların çalışmalarını takip ederek hem bu grupların tüm kullanıcılarına ulaşmalarında hem de AB vatandaşlarına güvenlik hizmetlerinin sunulmasının geliştirilmesinde üye ülkelere yardımcı olmayı amaçlamaktadır. Dolayısıyla bu bağlamda ENISA'nın üstlendiği role bakıldığında, STİM alanındaki küresel oyuncularla temas içerisine girdiği görülmektedir. FIRST, TF-CSIRT, CERT/CC, APCERT ve CNCERT/CC temsilcileri ile görüşmeler gerçekleştirmiştir. Bunun yanı sıra İngiltere'deki WARP topluluklarını ziyaret ederek TERENA bünyesinde kurulan Transits ekibi ile işbirliği içinde eğitimler düzenlemiştir. Ajansın ayrıca etkinliklere ve konferanslara uzmanlık desteği verdiği de ifade edilmektedir (ENISA, 2011).

Sonuç olarak ENISA, ağ ve bilgi güvenliği alanındaki en uygulama örneklerini toplayarak bir STİM'nin nasıl kurulacağına ve işletileceğine ilişkin bilgileri yayınları aracılığıyla kullanıcılara ulaştırmaktadır (ENISA, 2011).

ENISA'nın STİM'lerin veya WARPs benzeri yapıların kurulmasını desteklemeye devam edeceği ifade edilmektedir. Bunun yanı sıra bu yapıların sundukları güvenlik hizmetlerinin kalitesini nasıl arttırabileceklerine ilişkin önlemlerin de ENISA tarafından denetlenmesi öngörülmektedir. Ajansın üye devletlere ülkelerindeki bilgi teknolojisi güvenliğinin arttırılmasına yönelik tavsiyelerde bulunması da hedeflenmektedir (ENISA, 2011).

Özetlemek gerekirse, gerek ITU tarafından hazırlanan GCA'da gerekse AB tarafından hazırlanan ADA'da, artan siber tehditlerle mücadele edilmesi amacıyla;

- Ülke düzeyinde siber güvenlik stratejisinin oluşturulması,
- Siber olayların yönetimini sağlayacak yapıların (U-STİM) kurulması,
- Kamu-özel sektör arasındaki işbirliğinin tesis edilmesi ve
- Uluslararası işbirliklerinin kurulması

gerekliliği vurgulanmaktadır.

Ülkemizde kurulucak U-STİM'in, STİM yapılarının kurulmasına destek veren, bu yapılara işbirliği ortamı sunarak siber tehditler ve bu tehditlerin bertaraf edilmesi amacıyla geliştirilen çözüm önerileri konularında bilgi paylaşımına imkân veren IMPACT, FIRST ve ENISA gibi uluslararası platformlarda aktif bir şekilde yer alması gerektiği değerlendirilmektedir.

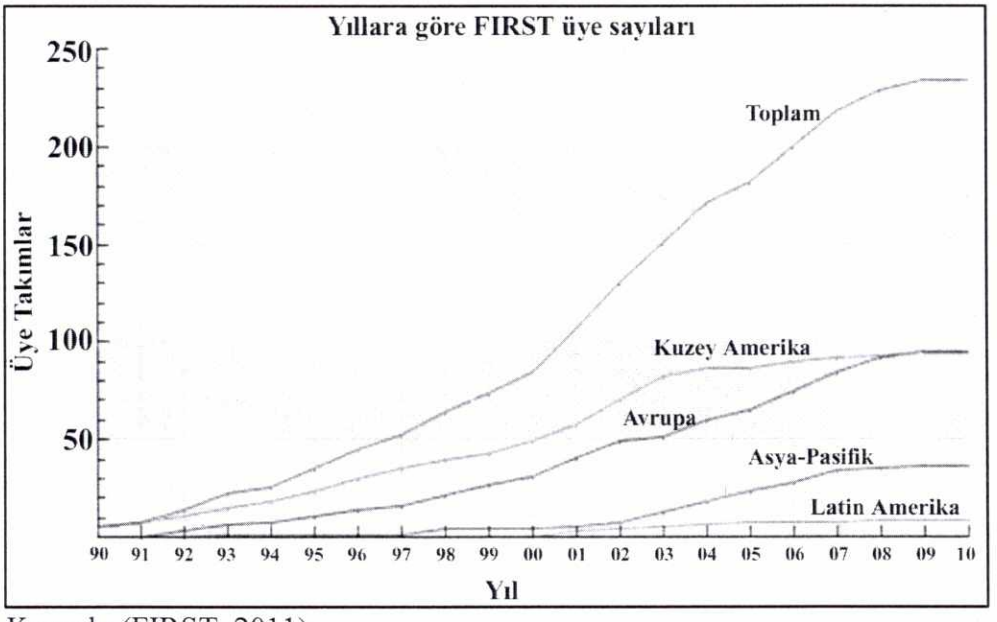
3.3. FIRST

1988 yılında "internet solucanı" olarak bilinen bir bilgisayar güvenlik olayı meydana geldiği, bu olaya karşı alınan önlemlerin etkili olmadığı ve getirilen çözüm önerilerinin farklı farklı olduğu bilinmektedir. Bu olaydan haftalar sonra CERT/CC, sonrasında ise kendisinden hizmet alan kurum/kuruluşlara hizmet vermek amacıyla ABD Enerji Bakanlığı bünyesinde Bilgisayar Olayları Danışma Birimi (Computer Incident Advisory Capability-CIAC) kurulmuştur (FIRST, 2011).

Sonraki iki yıl boyunca, belirli bir hedefi, mali yapısı ve müşteri yelpazesi olan siber olaylara müdahale ekiplerinin sayısının artmaya devam ettiği görülmektedir. Dilin, zaman diliminin, uluslararası standartların veya sözleşmelerin farklı olması siber olaylara müdahale ekipleri arasındaki ilişkilerde birçok sorunun yaşanmasına neden olmuştur. 1988 yılında ortaya çıkan "Wank solucanı" ile yaşanan güvenlik olayı söz konusu ekipler arasındaki haberleşmenin ve koordinasyonun öneminin anlaşılmasına sebep olmuştur. Bir çözüm geliştirilmesi gerektiğinden hareketle 1990 yılında FIRST kurulmuştur (FIRST, 2011).

Dünya çapında siber olaylara müdahale ekiplerinin kurulmaya devam ettiği ve sayılarının arttığı görülmektedir. FIRST eğitim, ticaret, üretim, devlet ve askeri alanından birçok üyesi bulunan bir STİM işbirliği platformu olarak hizmet vermektedir. Üye sayısının 2010 yılında 250'ye yaklaştığı görülmektedir (Şekil 3.1).

Şekil 3.1. FIRST - üye sayısı (1990–2010)



Kaynak: (FIRST, 2011)

3.3.1 Vizyonu ve misyonu

FIRST, üyelerine siber olaylara müdahale alanında uluslararası işbirliği imkânı sunan ve dünya çapında lider kabul edilen öncü bir kuruluş olarak hizmet vermektedir. FIRST'e üye olan STİM'lere, en iyi uygulama örneklerine ve müdahale araçlarına erişme, diğer üyelerle güvenli bir şekilde haberleşme hizmeti sunulmakta ve siber tehditlerle daha etkin bir şekilde mücadele etme imkânı verilmektedir (FIRST, 2011).

Güvenilen STİM'lerden oluşan ve işbirliği içinde siber olayları ele alan bir konfederasyon olarak FIRST'ün, üyelerine sunduğu imkânlar arasında:

- Teknik bilgi, teknik müdahale araçları, metodolojiler ve süreçler geliştirmek ve bunları paylaşmak,
- Kaliteli güvenlik ürünlerinin, politikalarının ve hizmetlerinin geliştirilmesini teşvik etmek ve desteklemek,
- En iyi siber olaylara müdahale uygulamalarını geliştirmek ve bunları yayımlamak,
- Siber olaylara müdahale ekiplerinin oluşturulmasını, büyümesini ve dünyanın dört bir yanındaki kuruluşların FIRST'e üye olmalarını desteklemek ve

- Tüm üyelerin bilgi birikimini, becerilerini ve tecrübelerini kullanarak daha güvenli bir elektronik ortamın oluşmasını teşvik etmek

yer almaktadır (FIRST, 2011).

3.3.2 Politikaları

FIRST, siber olaylarla ve tehditlerle mücadele konusunda gönüllü olarak çalışan STİM'lerden oluşan bir işbirliğidir. FIRST yönetim kurulu tarafından belirlenerek üyeliğe kabul edilen ekipler devlet, kolluk, akademi, özel sektör ve diğer farklı alanlarda faaliyet gösteren çeşitli kuruluşları temsil etmektedirler (FIRST, 2011).

Yönetim kurulu tarafından her yıl gözden geçirildiği ifade edilen vizyon ve misyon konusundaki değişikliklerin ve önerilerin genel kurul toplantısında veya yapılan ilave toplantılarda yönetim kurulunun 2/3 çoğunluğu ile kabul edilmesi gerekmektedir.

Tam üye olmak isteyen STİM'lerin mevcut iki tam üye tarafından aday gösterilmesi gerekmektedir. İhtiyaç duyulması halinde aday göstermek için yönetim kurulunun kararı ile mevcut bir üye de yeterli kabul edilebilmektedir. İlişkili kuruluş olmak isteyen STİM'lerin ise mevcut bir tam üye tarafından aday gösterilmesi gerekmektedir. Tüm adaylıkların yönetim kurulunun tüm üyelerinin 2/3 oyu ile kabul edilmesi zorunlu koşulmaktadır. Yönetim kurulunun üyeliğini kabul ettiği üyenin üyelik ücreti ödemesi gerekmektedir (FIRST, 2011).

Üye veya ilişkili kuruluş olmak üzere önerilen STİM'ler adaylıklarını desteklemek üzere aşağıda belirtilen bilgileri sağlamalıdırlar (FIRST, 2011):

- Grubun, organizasyonun veya bireyin adı veya kimliği,
- FIRST'e katılma nedeni,
- Adayın katılımının FIRST'e sağlayacağı yararlar,
- Üyenin veya ilişkili kuruluşun irtibat noktası,
- Üyeler için, adayın hizmet vereceği kurum/kuruluşlara ilişkin açıklamalar,
- İlişkili kuruluşlar için, adaylık için sponsor olan üye takım ve

- Katılım profilinin belirlenmesi için her ekipten istenen diğer bilgilerin tamamlanması.

Aday olan ekibin tam üyeliğe kabul edilebilmesi için adaya üyelikte sponsor olan en az bir tam üyenin aday ekibin tesislerine bir ziyaret gerçekleştirmiş olması şartı aranmaktadır. Adaya destek veren tüm sponsorların talebi ve yönetim kurulunun tüm üyelerinin 2/3 oyu ile kabul edilmesi durumunda ziyaret ihmal edilebilmektedir. Yıllık aidat ödendiği, üyeliği iptal ettirecek bir durum olmadığı veya ekibin kendisi gönüllü olarak üyelikten çıkmak istemediği sürece FIRST üyeliği devam etmektedir (FIRST, 2011).

Herhangi bir katılımcı istediği zaman FIRST üyeliğinden vazgeçebilmekte, bu şekilde üyeliği sona eren ekiplere üyelik aidatı geri ödenmemektedir (FIRST, 2011).

Aşağıda yer verilen durumlardan herhangi birinin vuku bulması durumunda yönetim kurulu üyeliği iptal edilmesi işlemlerini başlatmaktadır (FIRST, 2011):

- Üyelik şartlarına uyum sağlanmadığında,
- İşbirliği eksikliğinde,
- FIRST'ün amaç ve hedeflerine uygun hareket edilmediğinde,
- Belirlenen süre içerisinde FIRST üyelik aidatının ödenmesinde aksaklıklar olması,
- Aktif bir tam üyenin sponsor olarak belirlenmesinde sorun yaşanması,

Hakkında üyelik iptali işlemi başlatılan katılımcının FIRST'ün imkânlarına ve hizmetlerine erişimi askıya alınabilmektedir. Askıya alınma veya iptal edilme kararı yönetim kurulunun tüm üyelerinin 2/3 oyunu gerektirmektedir. Katılımcıya iptal konusu ile ilgili savunma hakkı da verilmektedir. Askının kaldırılması ve üyeliğin yeniden aktive edilmesi de yine yönetim kurulunun tüm üyelerinin 2/3 oyuna bağlanmaktadır. Herhangi bir sebeple üyelikleri askıya alınan veya iptal edilen üyelerin üyelik aidatları geri ödenmemektedir (FIRST, 2011).

Üyelik ücretleri yönetim kurulu tarafından belirlenmekte ve gözden geçirilmektedir. Gerek görülmesi durumunda üyelik ücretlerinin ödeneceği tarih aralıkları da değiştirilebilmektedir. Üyelik ücretinin yapısının da yönetim kurulunun çoğunluğunun 2/3 oy oranı ile kabul edilmektedir. Gelirlerdeki artışın hesaplanabilmesi amacıyla mevcut ve yeni belirlenen üyelik ücretleri genel kurul toplantısının yapıldığı anda üyelere uygulanmaktadır. Bir üyenin veya ilişkili kuruluşun FIRST'ün üyelik ücretine denk veya daha fazla miktarda bir bağış ya da sponsorluk sağlaması durumunda yıllık üyelik aidatından feragat edilebilmektedir (FIRST, 2011).

Siber tehditlerle mücadele eden dünyanın farklı yerlerindeki STİM'lerin gönüllü olarak çalıştıkları, üyeleri arasında devlet, kolluk, akademi, özel sektör ve diğer farklı alanlardan STİM'lerin bulunduğu bir platform olan FIRST, U-STİM'lerin uluslararası işbirliği ihtiyacına cevap verebilecek nadir kuruluşlardan biridir. Üyelerine siber olaylara müdahale alanında uluslararası işbirliği imkânı sunan ve dünya çapında lider kabul edilen bir kuruluş olarak hizmet veren FIRST'e üye olan STİM'lerin, siber tehditlere müdahalede en iyi uygulama örneklerine ve müdahale araçlarına erişme imkânı bulunmaktadır.

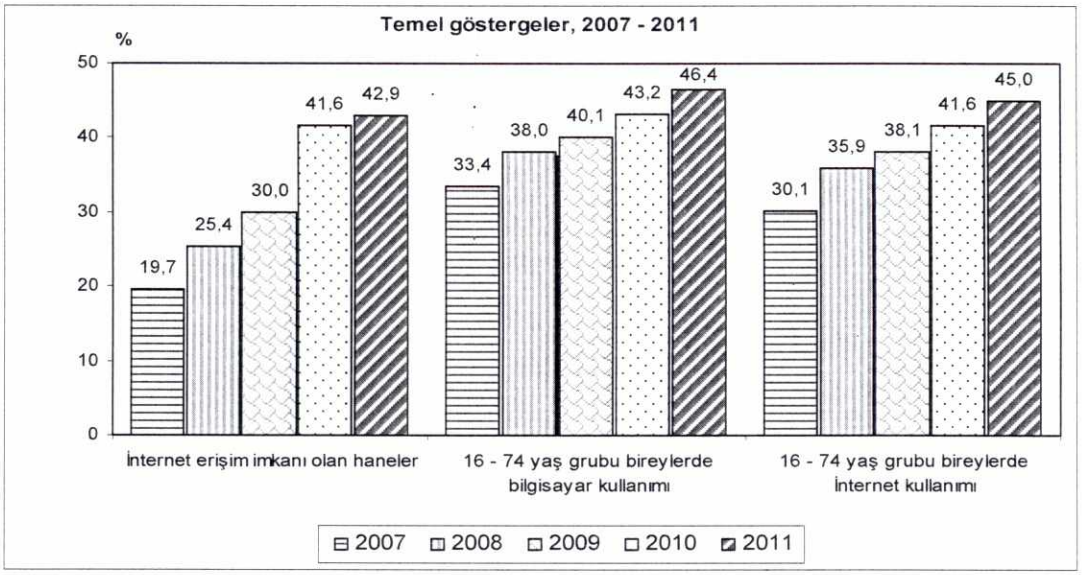
4. TÜRKİYE İNCELEMESİ

BİT'lerin sağladığı fırsatların toplumun neredeyse tüm kesimlerine ulaştığı günümüzde, kişiler gündelik ve iş hayatlarında bu teknolojileri yaygın bir biçimde kullanmaktadır. Dünyadaki bu gelişmelerin ülkemizde de kaydedildiği görülmektedir.

4.1. Bilgi ve iletişim teknolojileri

Türkiye İstatistik Kurumu (TÜİK) verilerine göre ülkemizde 2011 yılı itibariyle internet erişim imkânı olan hane oranı % 42.9'a, 16-74 yaş grubu bireylerde internet kullanımı ise %45.0'e (TÜİK, 2011) ulaşmıştır (Şekil 4.1).

Şekil 4.1. Yıllara göre hanelerde BİT kullanım oranları



Kaynak: TÜİK

İnternet kullanımının artışına paralel olarak internet üzerinden kişisel kullanım amaçlı alış verişin de 2010 yılına oranla 2011 yılında artış gösterdiği görülmektedir. 2010 yılında oranı %15 olan internet üzerinden mal veya hizmet siparişi vermenin veya satın almanın 2011 yılında %18,6 oranına ulaştığı belirtilmektedir (TÜİK, 2011).

Ağustos 2009–2010 tarihleri arasında kişisel amaçla interneti kullanan bireylerin yarısına yakınının (%46.8) bir güvenlik problemi ile karşılaştığı ifade edilmektedir. Karşılaşılan problemler arasında ilk sırada %36.4 ile virüs veya diğer bilgisayar sorunları, %32 ile ise istem dışı elektronik postaların yer aldığı görülmektedir (TÜİK, 2010a).

Girişimlerin internet erişimi sahipliğine bakıldığında, 10 ve daha fazla çalışanı olan girişimlerin %90,9'unun, 250 ve üzeri çalışanı olan girişimlerde %98,4'ünün, 50–249 çalışanı olan girişimlerin ise %96,9'unun internet erişimine sahip olduğu tespit edilmiştir (TÜİK, 2010b).

4.2. Siber tehditler ve olaylar

Gerçek dünyada işlenen suçlar kadar suçun, fiziksel ortamda var olan tehditler kadar tehdidin sanal ortamda olduğunu ve kullanıcıları tehdit ettiğini söylemek mümkündür. Dünyada 2011 yılının ilk yarısında her 4.5 saniyede bir internet tehdidinin ortaya çıktığı, günlük 150.000 kötücül yazılım örneğinin tespit edildiği görülmektedir (Sophos, 2011). Stuxnet, endüstriyel kontrol sistemlerindeki güvenlik açıklıklarını kullanarak sabote etmek için özel tasarlanan silahlandırılmış ilk kötücül yazılım olarak kabul edilmektedir. Belirli bir ürünün kontrol sistemlerini hedef alan Stuxnet, İran'ın uranyum zenginleştirme programını önemli oranda etkilemiştir (PWC, 2011). Dolayısıyla ülkemizdeki kritik altyapıların kontrol sistemlerinin çok büyük tehdit altında olduğunu söylemek mümkündür.

Siber tehditler siber suça dönüşerek birçok kullanıcıyı, organizasyonu, kamu kurumunu ve devleti çeşitli zararlara uğratmaktadır. Artan siber tehditlere artan güvenlik açıklıklarının eklenmesi ile siber saldırılar da artmaktadır. Bu saldırılardan ülkemizin de önemli ölçüde etkilendiği, birçok saldırının hedefi veya kaynağı olduğu görülmektedir.

Türkiye'de ağustos ayında uygulamaya konulması planlanan güvenli internet projesine karşı, kendilerini uluslararası bilgisayar aktivistleri olarak tanıtan

Anonymous, 9 Haziran 2011 tarihinde Telekomünikasyon İletişim Başkanlığı'nın (TİB) sistemlerine 100 bin köle bilgisayar ile saldırı gerçekleştirmiştir. Ancak TİB'in sistemleri devre dışı bırakılamadı (Bugün, 2011).

9 Haziran 2011 günü saat 17:50 itibari ile başlayan saldırının, saat 19:15'te 2 Gbps hızına çıktığı, 22:00'de ise 4 Mbps hızına düştüğü ifade edilmektedir. Saldırı süresince TİB'in sistemlerine erişimde herhangi bir problemin yaşanmadığı da belirtilmektedir (BTK, 2011).

Söz konusu saldırıya ülke dışından katılan saldırganlara yönelik gerekli önlemlerin alınmasına paralel olarak ülke içinden saldırıya katılanlara ilişkin elde edilen bilgiler adli ve idari birimlerle paylaşılmıştır (BTK, 2011).

2010 yılının ilk çeyreğinde üst düzey alan adlarını hedef alan SQL enjeksiyonu saldırısında *".tr"* alan adı ile Türkiye'nin ilk sırada (Microsoft, 2010) yer aldığı görülmektedir (Tablo 4.1).

Tablo 4.1. SQL enjeksiyonu saldırısına maruz kalan ilk 5 üst düzey alan adı

Sıra	Üst düzey alan adı	Mağdur sayfa sayısı
1	.tr	88,378
2	.com	43,144
3	.org	18,331
4	.net	5,206
5	.ru	5,179

Kaynak: Microsoft

Genellikle kullanıcısının haberi olmadan bilgisayara bulaşan, o bilgisayarı köle bilgisayar yapan ve bir KBA'ya dâhil eden kötücül yazılımlar en büyük siber tehditler arasında sayılmaktadır. Ülkemizde 2009 yılının son iki çeyreğinde ve 2010 yılının ilk çeyreğinde bilgisayarları bir KBA'ya dâhil eden kötücül yazılım bulaşma oranlarının dünya ortalamasının üstünde olduğu (Microsoft, 2010) görülmektedir (Tablo 4.2).

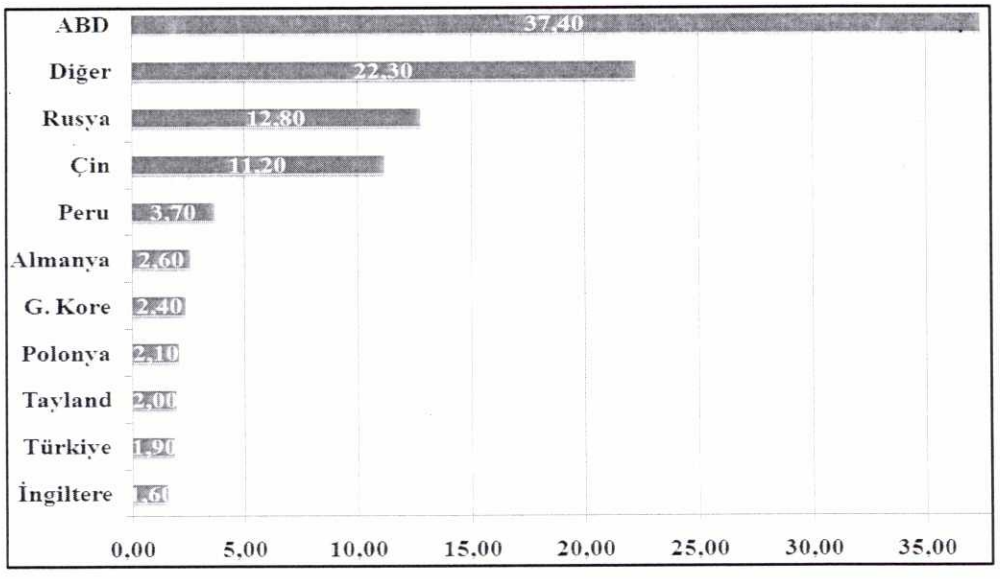
Tablo 4.2. Kötücül yazılım bulaşma oranları

Ülke	2009/3. Çeyrek	2009/4. Çeyrek	2010/1. Çeyrek	2010/2. Çeyrek
Hollanda	2.8	2.0	4.6	2.5
Çin	1.4	1.0	1.3	1.0
Avustralya	2.4	2.4	3.4	2.8
ABD	5.9	4.5	5.6	5.2
Türkiye	4.1	2.8	5.8	4.7
Dünya ortalaması	2.5	2.5	4.0	3.2

Kaynak: Microsoft

Kötücül yazılıma kaynaklık eden ülkeler sıralamasında 2010 yılında Türkiye'nin %1.90 ile ilk 10 ülke arasında 9 uncu sırada (Sophos, 2010) yer aldığı görülmektedir (Şekil 4.2).

Şekil 4.2. İnternette kötücül yazılım barındıran ilk 10 ülke



Kaynak: Sophos

2010 yılında kötücül yazılım bulaşma sıralamasında Türkiye'nin yine ön sıralarda yer aldığı görülmektedir. Türkiye'de 2010 yılının son çeyreğinde günde ortalama 32.8 bilgisayardan kötücül yazılım temizlendiği güvenlik raporlarına yansımaktadır.

Kötücül yazılım temizlenen bilgisayar sayısında bütün yıl boyunca ise 36.8'lik bir ortalama değerle Türkiye'nin ilk sırada yer aldığı görülmektedir (Microsoft, 2011).

Bir güvenlik firması olan AVG tarafından 144 ülkeden 127 milyon bilgisayara ait verilerin derlendiği araştırma raporuna göre, 2010 yılında barındırdıkları çevrimiçi tehditlere göre ülkeler sıralamasında Türkiye ilk sırada yer almaktadır (AVG, 2010). Rapora göre Türkiye'de her on kullanıcıdan biri herhangi bir siber tehdide maruz kalmaktadır. Söz konusu raporda internete bağlanmak için en riskli ülke olarak da yine Türkiye gösterilmektedir (Tablo 4.3).

Tablo 4.3. İnternete bağlanmak için en riskli ülkeler

Ülke	**Tehdide maruz kalan kullanıcı sayısı**
Türkiye	1 / 10
Rusya	1 / 15
Ermenistan	1 / 24
Azerbaycan	1 / 39
Bangladeş	1 / 41

Kaynak: AVG

Söz konusu araştırma her ne kadar kullanıcıları risk altında olan ülkeleri ortaya koyuyor olsa da internet üzerindeki tehditlerin sınır tanımaz yapısı aslında bütün ülkeleri endişelendirmektedir.

Ülkemiz istem dışı elektronik postaya kaynaklık eden ülkeler sıralamasında 2010 yılının öncesinde genellikle ilk üçte bazen de ilk sırada yer alıyordu. İstem dışı elektronik postaya kaynaklık etmede internet tarihinde ilk defa 2010 yılında tüm dünyada ve Türkiye'de 2009 yılına oranla bir azalma görülmesine rağmen Avrupa'da artış görülmüştür (Tablo 4.4).

Tablo 4.4. İstem dışı elektronik postadaki durum 2009–2010

Ülke	2010 (Trilyon/Yıl)	2009 (Trilyon/Yıl)	Fark
ABD	11.1	11.3	-1.6%
Hindistan	9.1	6.4	40.7%
Brezilya	7.0	13.3	-47.5%
Rusya Federasyonu	6.4	5.0	27.7%
Vietnam	4.3	5.6	-22.4%
Polonya	3.6	3.8	-5.9%
Çin	3.6	4.2	-13.5%
İngiltere	3.6	1.8	98.9%
Ukrayna	3.4	2.4	45.4%
Fransa	3.0	1.4	115.3%
Almanya	2.8	2.6	10%
Türkiye	**.45**	**3.7**	**-87%**

Kaynak: Cisco

Ülkemizde 2009 yılının ikinci yarısında hayata geçirilen istem dışı elektronik postaların önlenmesine ilişkin projenin Türkiye'de 2010 yılında istem dışı elektronik postadaki azalmada önemli katkısının olduğu değerlendirilmektedir.

Türkiye siber âlemde sadece saldırılara hedef olan, kötücül içerikleri ve faaliyetleri barındıran ülkeler arasında yer almamaktadır. Gelişen ve yaygınlaşan BİT'ler ülkemizin zaman zaman saldırıların kaynağı olmasına da yol açmaktadır. 2011 yılının ilk çeyreğinde Ermeni soykırımının uluslararası alanda tanınma sürecine karşı Türk korsanlar tarafından büyük bir kampanya başlatılmış ve 6.173 adet Ermeni internet sayfasına saldırı düzenlenmiştir (McAfee, 2011).

Ülkemizde siber ortamda işlenen suçlara bakıldığında en çok işlenen bilişim suçları sıralamasında 1132 adet olayla banka ve kredi kartı dolandırıcılığının (KOM, 2011) ilk sırada yer aldığı görülmektedir (Tablo 4.5).

Tablo 4.5. 2010 yılında meydana gelen olay ve şüpheli sayıları

Olay Türü	Olay	Şüpheli
Banka ve Kredi Kartı Dolandırıcılığı	1132	1005
İnteraktif Banka Dolandırıcılığı	151	300
Bilişim sistemlerine girme, engelleme, bozma, verileri yok etme, değiştirme	975	1351
İnternet Aracılığıyla Nitelikli Dolandırıcılık	71	115
Diğer	28	134
Toplam	2357	2905

Kaynak: KOM

4.3. Yapılan çalışmalar

Ülkemizde BİT'ler hızlı bir şekilde yaygınlaşmakta, buna paralel olarak kaynağı veya hedefi Türkiye olan kötücül faaliyetler ve siber tehditler de artış göstermektedir. Bu bağlamda ülkemizde genelde siber güvenlik özelde ise kötücül faaliyetler ve siber tehditler konusunda yapılan çalışmalara bakıldığında;

- 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi Eylem Planının "Ulusal Bilgi Sistemleri Güvenlik Programı" başlıklı 88 inci Eylemi ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne (UEKAE) bilgisayar olaylarına müdahale ekibi kurma görevi verilmiş, bu görev kapsamında Türkiye Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) kurulmuştur (BTK-TÜBİTAK, 2011).
- 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nda:
    - Kurum tarafından yapılacak düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi ilkesi,
    - Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak konusunda BTK'ya görev ve yetki verilmesi [Madde 6 ş bendi],

- Kişisel veri ve gizliliğin korunması ve izinsiz erişime karşı şebeke güvenliğinin sağlanması konusunda işletmecilere yükümlülük getirilmesi [Madde 12 d ve j bentleri].

yer almaktadır (EHK, 2008).

- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu ile:
  - 10 uncu maddesinin dördüncü fıkrasının d bendinde ifade edilen "İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dâhil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak" [Madde 10, 4 üncü fıkra, d bendi]

konusu düzenlenmiştir. Ayrıca BTK bünyesinde gerek EHK kapsamında gerekse ITU nezdinde çeşitli çalışmalar yürütülmektedir.

Ülkemizde siber suçlarla mücadelenin tarihi 1990'lı yılların sonlarına dayanmaktadır. Emniyet Genel Müdürlüğü (EGM) Bilgi İşlem Dairesi Başkanlığı bünyesinde 1997 yılında oluşturulan bir büro amirliği ile siber suçlarla mücadelede ilk kurumsal yapılanma gerçekleştirilmiştir. 2011 yılının Temmuz ayına kadar ki sürede ise, EGM bünyesinde Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanlığı bünyesinde yer alan Bilişim Suçları İle Mücadele Şube Müdürlüğü siber suçlarla mücadele etmektedir (Demir ve Küçükuysal, 2011). 2011 yılı Temmuz ayında Bakanlar Kurulu Kararı ile EGM bünyesinde bir daire başkanlığı kurulması kararlaştırılmıştır (Resmi Gazete, 2011). Söz konusu daire başkanlığının Bilişim Suçları İle Mücadele Daire Başkanlığı olarak hizmet vereceği ifade edilmektedir (Şen, 2011).

Siber olaylar meydana geldikten sonra olayın soruşturulması safhasında kolluk kuvvetleri meydana gelen olaya ilişkin çeşitli delillere ihtiyaç duymaktadır. Bu delillerin siber olaydan etkilenen kurum ve kuruluşlardan temin edilmeye çalışılmasının yanı sıra, hizmet veren U-STİM aracılığıyla elde edilmeye çalışılması da söz konusu olabilmektedir. Zira soruşturma ve yargılama safhalarında kullanılmak

üzere delillerin U-STİM tarafında da bulunabilmesi teknik olarak mümkün olabilmektedir. Her ne kadar saldırıya hedef olan kurumdaki verilere doğrudan erişim sağlanamasa da mevcut bağlantılardan elde edilen veya bahse konu kuruma giden bağlantıların analizinden saldırı veya suça ilişkin bilgiler elde edilebilmektedir. Ancak ülkemizde kolluk ile TR-BOME arasında bu tür bir bilgi paylaşımının umulan seviyede olmadığı anlaşılmaktadır. Suçun soruşturulması aşamalarında TR-BOME'nin de ülkemizdeki kurumların STİM anlayışının da yavaş yavaş gelişmeye başladığı ve umulan seviyeye ulaşmak için daha fazla çalışmaya ihtiyaç olduğu ifade edilmektedir (Şen, 2011).

Ayrıca, KOM'da bankacılık konularında uzman polislerin olduğu, bu personelin bankalarla zaman zaman bir araya geldikleri ve siber suçlar konusunda edindikleri bilgi ve deneyimleri bankalarla paylaştıkları da belirtilmektedir (Şen, 2011). Benzer bir şekilde kolluk ile U-STİM arasında olması gereken işbirliğinin bir gereği olarak, siber olaylar konusunda uzman KOM personelinin U-STİM ile de düzenli bir bilgi alış verişinde bulunması gerektiği de değerlendirilmektedir.

Özetlemek gerekirse, BİT'lerin yaygınlaşması, kötücül faaliyetlerin artması, mobil teknolojilerin giderek yaygınlaşması da dikkate alındığında, siber olaylara kaynaklık etme ve siber tehditlerin hedefi olma konusundaki veriler değerlendirildiğinde, ülkemizin siber güvenlik ihtiyacının giderek arttığını, bu ihtiyacın karşılanması amacıyla ulusal düzeyde tüm tarafları bir araya getirecek çalışmalar yapılması gerektiği görülmektedir.

Kötücül Yazılımlarla Mücadele Projesi (KYMP), Ulak-CSIRT, TR-BOME ve Ulusal Siber Güvenlik Tatbikatı – 2011 (USGT-2011) ülkemizde siber tehditlerle ve olaylarla mücadele konusunda yapılan çalışmalar arasında yer almaktadır.

4.3.1 Kötücül yazılımlarla mücadele projesi (KYMP)

İstatistikler incelendiğinde siber tehditlere ve siber saldırılara en fazla kötücül yazılımların kaynaklık ettiği gözlemlenmektedir. Kötücül yazılımlar içerisinde ise, bir bilgisayarı sahibinin haberi olmadan kullanarak köleleştiren köle bilgisayar

yazılımlarının (BOT) yaygın bir şekilde kullanıldığı bilinmektedir. Kötücül faaliyet yürütenler binlerce hatta bazen milyonlarca bilgisayarı köleleştirerek köle bilgisayar ağları kurmaktadır. DDoS saldırılarının büyük bir kısmına kaynaklık eden KBA'lar, en büyük siber tehdit olarak görülmektedir. Bu endişeden hareketle genelde kötücül yazılımları özellikle de KBA tehdidine karşı dünyanın farklı ülkelerinde farklı çalışmalar yürütülmektedir.

Almanya'da Alman İnternet Sanayi Derneği (Association of the German Internet Industry - ECO) tarafından Federal Bilgi Güvenliği Dairesi'nin (Bundesamtes für Sicherheit in der Informationstechnik - BSI) de desteği de alınarak Anti-Botnet-Danışmanlık Merkezi kurulmuştur. Merkez İSS'lerle işbirliği içinde çalışmaktadır (BOTFREI, 2011).

Federal İçişleri Bakanlığı tarafından finanse edilen merkezin;

- Bilgilendirme,
- Temizleme ve
- Önleme

olmak üzere çalışmalarını üç başlık altında topladığı görülmektedir. Söz konusu çalışmalarla, köle bilgisayar yazılımları konusunda kullancıların bilinç düzeyinin arttırılması, kullanıcının sistemine bulaşan kötücül yazılımların temizlenmesinde kullanıcıya yardımcı olunması ve kötücül yazılımların gelecekte bulaşmasının önlenmesi amaçlanmaktadır. Bu amaçlarla kullanıcılara telefonla destek hizmeti verilmektedir (BOTFREI, 2011).

Benzer bir şekilde Japonya'da internet için bir tehdit olan BOT yazılımlarının;

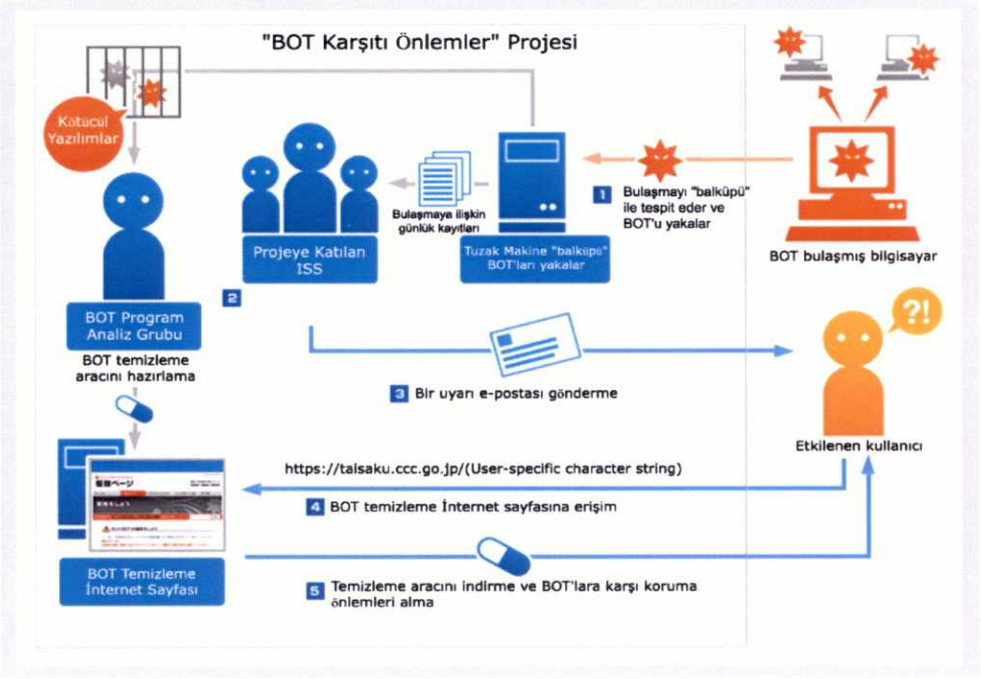
- Karakteristiklerini incelemek,
- Bilgisayarlara bulaşmasını engellemek ve
- Bulaşmış ise temizlenmesini sağlamak

üzere Japonya'da BOT Karşıtı Önlemler Projesi başlatılmıştır. Proje kapsamında 2006 yılında Siber Temizlik Merkezi (Cyber Clean Center - CCC) kurulmuştur (CCC, 2011).

İçişleri ve iletişim Bakanlığı ve Ekonomi Ticaret ve Endüstri Bakanlığının yönetiminde yer aldığı CCC'de, operasyon grubu, analiz grubu ve tanıtım grubu adı altında çalışmalar yürütülmektedir. Projeye çok sayıda İSS destek vermektedir (CCC, 2011).

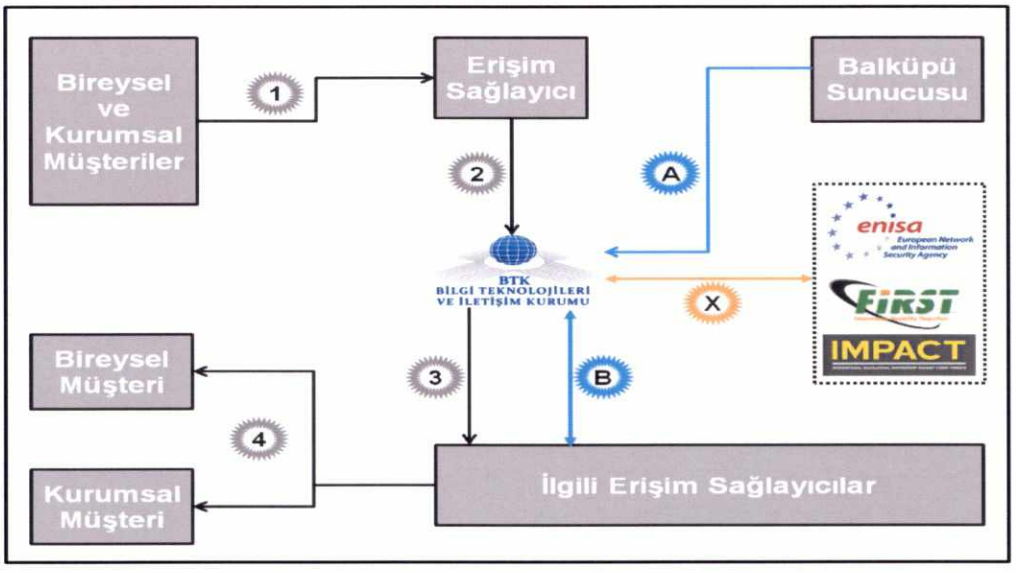
CCC işlem döngüsünde öncelikle BOT elde edilmekte, etkilenen kullanıcıların tespit edilmesi amacıyla söz konusu BOT'un sistemlere bulaşmasına ilişkin günlük kayıtları projeye katılan İSS'lerle paylaşılmakta, analiz grubu tarafından analiz edilen BOT yazılımını temizleyen bir araç geliştirilerek (CCC, 2011) kullanıcıların kullanımına sunulmaktadır (Şekil 4.3).

Şekil 4.3 Japonya - Siber temizlik merkezinin işlem döngüsü



Kötücül yazılımlar kullanılarak gerçekleştirilen saldırılardan ve oluşan tehditlerden ülkemizin de önemli oranda etkilendiğinin gözlemlenmesinden hareketle, bu yazılımlarla mücadele edilmesi ihtiyacı ortaya çıkmıştır. Bu ihtiyaca cevap verebilmek amacıyla, kötücül faaliyetlere ve KBA'lara karşı dünyada yürütülen faaliyetler araştırılmış, özellikle Almanya'da ve Japonya'da hayata geçirilen çalışmalar incelenmiş ve BTK bünyesinde KYMP projesi başlatılmıştır (Şekil 4.4).

Şekil 4.4 KYMP



KYMP projesi kapsamında kapsamında ülkemizde;

1. Saldırıya uğrayan kullanıcının hizmet aldığı erişim sağlayıcıya başvurması ve kendisine saldırıda bulunan IP adreslerini bildirmesi,
2. Erişim sağlayıcının, sistemlerindeki ilgili trafik hacmini inceleyerek saldırı olasılığını teyit etmesini ve
   - Müşterilerinden aldığı ve teyit ettiği saldırgan IP adreslerini,
   - Erişim sağlayıcının kendisine bir saldırı yapılmışsa saldıran IP adreslerini,
   - Herhangi bir yolla edindiği saldırgan IP adreslerini

   BTK'ya iletmesi,
3. BTK'nın, kendisine iletilen IP adreslerini erişim sağlayıcılara göre ayrıştırırak saldırı olasılığı bilgisini ve ilgili IP adreslerini ilgili erişim sağlayıcılara iletmesi, saldırgan IP adresinin yurtdışından olması halinde bu IP adreslerini yurtdışı çıkışı olan erişim sağlayıcılara iletmesi,
4. Erişim sağlayıcıların kendilerine iletilen IP adreslerinin tahsisli olduğu;
   - Kurumsal müşterilerin temas noktasını konu hakkında bilgilendirmesi ve tedbir almaya davet etmesi,
   - Bireysel müşterilerin internet bağlantılarını anlık olarak kesmesi ve uyarıcı bilgilerin yer aldığı bir internet sayfasına yönlendirmesi

A. Gönüllü erişim sağlayıcıların, kuracakları balküpü sunucuları ile KBA'nın komuta kontrol sunucularını belirlemeye olanak sağlayan "bot" yazılımlarını elde etmeleri ve bu yazılımları inceleyerek komuta kontrol sunucularına erişim sağlayacak bilgilere elde etmeleri,

B. Gönüllü erişim sağlayıcıların elde ettikleri bilgileri BTK'ya iletmeleri ve BTK'nın bu bilgileri gerekli tedbirleri almaları için erişim sağlayıcılara iltmesi ve

X. BTK'nın, kötücül yazılımlarla mücadele eden ENISA, IMPACT ve FIRST gibi uluslararası kuruluşlarla bilgi paylaşımında bulunması

hedeflenmektedir.

Kötücül faaliyetlere karşı yürütülen mücadelelerde uluslararası işbirliğinin öneminden dolayı söz konusu proje kapsamında uluslararası işbirliği platformu IMPACT' üye olunmuştur.

Proje kapsamında tehditlerin toplanması, analiz edilmesi ve sistemlere işlenmesi, İSS'lerle bilgi paylaşımında bulunulması süreçlerinin yönetiminde kullanılacak bir platform geliştirilmiştir. Bu bağlamda KYMP projesini ülkemizde etkin bir U-STİM yapısına geçiş aşaması olarak değerlendirmek mümkündür.

4.3.2 Ulak-CSIRT

Türkiye'de STİM konusunda yapılan çalışmalara bakıldığında, 2006 yılı Şubat ayında Ulusal Akademik Ağ (ULAKNET) Bilgisayar Olaylarına Müdahale Birimi (Ulak-CSIRT) kurulmuştur (ULAKBİM, 2011a). ULAKNET kapsamında kurulan bir güvenlik birimi olan Ulak-CSIRT, dış ağlardan ULAKNET'i hedef alan güvenlik ihlallerinin önlenmesinden, gerçekleşen saldırıların ve sorumlularının tespit edilmesinden, ULAKNET'ten dış dünyaya yapılan saldırıların önlenmesinden, oluşan saldırıların sorumlularının tespit edilmesinden ve bu bilgilerin ilgili ağ yöneticileriyle paylaşılmasından sorumludur (Ulak-CSIRT, 2011).

Ulak-CSIRT'ün amaçları:

- ULAKNET genelinde bilgi güvenliği bilincini arttırmak,

- Akademik ağı hedef alan siber olay sayısını azaltmak,
- Siber olay sorumlularını tespit etmek üzere koordinasyon çalışmalarını yürütmek,
- Sistem yöneticilerini güvenlik açıklıkları ve alınabilecek önlemler konusunda bilgilendirmek ve eğitim vermek,
- Bilgi güvenliği konusunda Türkçe doküman sağlamak

olarak sayılmaktadır (Ulak-CSIRT, 2011).

Ulak-CSIRT bünyesinde olay kayıtlarının merkezi bir şekilde oluşturulup takip edilmesi için Olay Takipçisi (OLTA) adlı bir uygulama geliştirilmiştir. OLTA vasıtasıyla olay kaydı sahibinin, olayı ihbar edenin ve Ulak-CSIRT'ün bilgilendirilmesi amaçlanmaktadır (ULAKBİM, 2011b).

Ulak-CSIRT 8 Temmuz 2007 tarihinde, Avrupa STİM Topluluğunun (CERT/CSIRT-Trusted Introducer) tüm şartlarını sağlayarak Trusted Introducer'e akredite olan Türkiye'nin ilk STİM ekibi olmuştur (ULAKBİM, 2011a).

4.3.3 TR-BOME

Ülkemizde STİM konusunda yapılan bir başka çalışma da TÜBİTAK UEKAE bünyesinde TR-BOME'dir. Devlet Planlama Teşkilatı Müsteşarlığı (DPT) Bilgi Toplumu Dairesi Başkanlığı tarafından hazırlanan Bilgi Toplumu Stratejisi Eylem Planı'nın 88 inci maddesinde yer alan Ulusal Bilgi Sistemleri Güvenliği Programında;

> Siber âlemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" kurulacaktır.
>
> Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır.

ifadeleri yer almaktadır (DPT, 2006). Söz konusu Plan'a dayanılarak, TÜBİTAK UEKAE bünyesinde TR-BOME Koordinasyon Merkezi (TR-BOME KM) kurulmuştur.

Görevi ülke genelinde kurum ve kuruluşlara bilgisayar güvenlik olaylarına müdahale yeteneği kazandırmak ve gerçekleşen bilgisayar güvenlik olaylarına müdahale etmek olarak ifade edilen ve ülkenin tamamına hizmet verme misyonu olan TR-BOME KM tarafından (TR-BOME, 2011);

- Olay müdahale koordinasyonu,
- BOME kurulum danışmanlığı ve
- Alarm-uyarılar

hizmetleri verilmektedir (TÜBİTAK-UEKAE, 2009).

4.3.4 BOME 2008 Tatbikatı

Kurumların güvenlik olaylarını tespit ve bu olaylara müdahale yeteneklerinin belirlenmesi amacıyla 2008 yılında TR-BOME KM'nin koordinatörlüğünde *"Bilgi Sistem Güvenliği Tatbikatı"* düzenlenmiştir. İki gün süren söz konusu tatbikata Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu ve Tapu Kadastro Genel Müdürlüğü olmak üzere 8 kamu kurumu katılmıştır (TÜBİTAK-UEKAE, 2008).

Kurumsal STİM süreçlerinin kontrol edilmesi ve yurt dışından kaynaklanan bir siber olayla karşı karşıya kalındığında işbirliği süreçlerinin kontrol edilmesi amacıyla gerçekleştirilen BOME 2008 tatbikatında, hayali bir ülkenin devlet başkanının ülkemize yapacağı bir ziyaret öncesinde bazı muhalif grupların söz konusu ziyareti protesto etmek için Türkiye'ye siber saldırı gerçekleştirme ihtimali senaryo olarak işlenmiştir (TÜBİTAK-UEKAE, 2008).

Tatbikat sonucunda çeşitli tespitler yapılmıştır (TÜBİTAK-UEKAE, 2008):

1. Tatbikat sürecindeki haberleşmenin tamamı imzalı ve şifreli olarak eposta üzerinden yapılmıştır. Ancak katılımcı kurumlardan bazılarının imzalı ve şifreli

elektronik posta gönderemediği bazılarının ise bu elektronik postaları açamadığı, bazı kurumların ise bu tür elektronik postaları engelledikleri tespitine yer verilmektedir. Dolayısıyla tatbikat sürecindeki haberleşmenin sağlıklı bir şekilde sağlanabilmesi için kullanılan şifreleme ve imzalama yazılımları gibi haberleşme bilgilerinin güncel olması gerektiği sonucuna varılmıştır.

2. Yapılan saldırıları tespit etmede kullanılan sistemlerin etkin olarak kullanılamadığı, bazı kurumların yapılan saldırıları bu sistemler tarafından kayıt altına alınmasına rağmen tespit edemedikleri görülmüştür. Dolayısıyla kayıt sistemlerinin etkin kullanımının siber olaylara müdahaleyi hızlandırdığı tespiti yapılmaktadır.
3. Siber olayın boyutlarının büyük olduğu durumlarda STİM ile iletişime geçmek ve işbirliği kurmak önemli bir adım olarak görülmektedir. Ancak 2008 tatbikatında bazı kurumların bu iletişimi kuramadıklarının tespit edildiği ifade edilmektedir.
4. Siber olaya kurum içinden yapılan müdahalelerin önceden belirlenmiş politika ve prosedürlere göre yapılmasının devamlılığı ve takip edilebilirliği sağladığı, ancak katılımcı kurumların siber olaya herhangi bir politikaya veya prosedüre göre tepki vermedikleri görülmüştür.
5. Bir siber olayın meydana geldiği sırada organizasyon içindeki koordinasyonun sağlanması olaya müdahalenin önemli gereklerinden biridir. 2088 tatbikatında katılımcı kurumların kurum içi koordinasyonu sağlamada sıkıntılar yaşadığı görülmüştür.

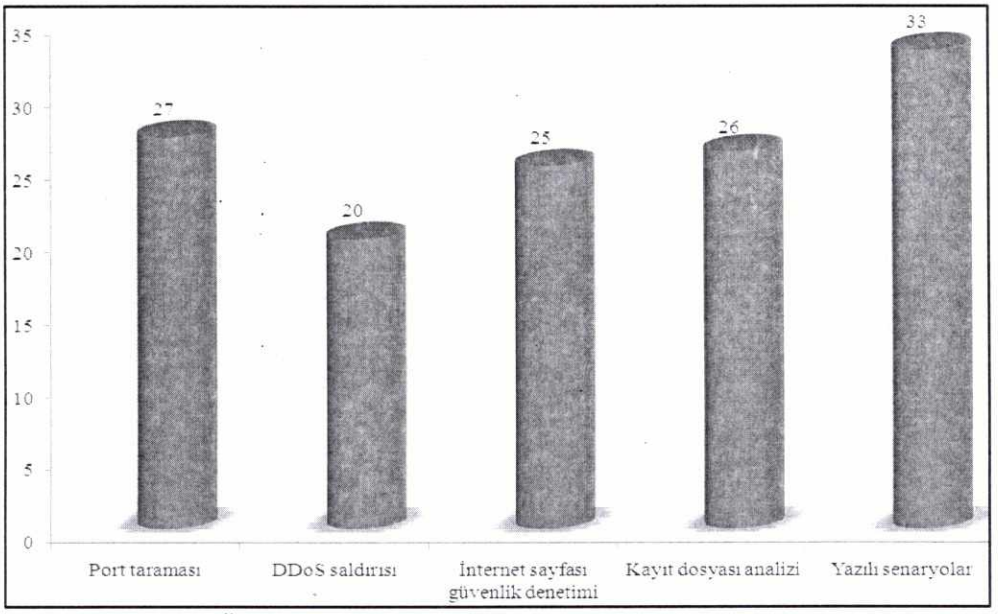
4.3.5 Ulusal siber güvenlik tatbikatı 2011 (USGT-2011)

Ulusal Siber Güvenlik Tatbikatı 2011 (USGT-2011), siber güvenlik alanında ülkemizdeki idari, teknik ve hukuki yeteneklerin arttırılması, bir siber olay esnasında kurum ve kuruluşlar arasındaki işbirliğinin geliştirilmesi, her kademede farkındalık oluşturulması ve kurum ve kuruluşların siber olaylara müdahale yeteneklerinin tespit edilmesi amaçlarıyla ve toplamda 42 kurum ve kuruluşun katılımı ile 25-28 Ocak 2011 tarihleri arasında gerçekleştirilmiştir (BTK-TÜBİTAK, 2011).

USGT-2011'e finans, BİT, eğitim, savunma ve sağlık alanlarından, adli birimlerden, kolluk kuvvetlerinden ve bazı bakanlıklardan temsilciler katılım sağlamıştır. Söz konusu tatbikatta bilişim, hukuk ve halkla ilişkiler uzmanı yaklaşık 200 temsilci görev almıştır (BTK-TÜBİTAK, 2011).

USGT- 2011'de teknik kabiliyetlerin tespit edilmesi, muhtemel siber olaylara müdahalede tecrübe kazandırılması amacıyla talep eden kurum ve kuruluşlara gerçek saldırılar yapılmış ve yazılı ortamda senaryolar gerçekleştirilmiştir (Şekil 4.5).

Şekil 4.5. USGT-2011'de gerçek saldırıların uygulandığı kurum kuruluş sayıları



Kaynak: BTK-TÜBİATK, 2011

USGT-2011'in ardından, çalışma süresince elde edilen veriler değerlendirilmiş ve:

1. Bazı kurumların bir bilgi güvenliği yönetim sistemine sahip olmadığı,
2. Sistem yöneticilerinin bazılarının siber güvenlik konusunda teknik olarak yeterli olmadığı,
3. Saldırı tespit sistemlerinin bazı kurumlarda kullanılmadığı, kullanılan bazı kurumlarda ise bu sistemlerden etkin bir şekilde yararlanılamadığı,

4. Güvenlik döngüsünün en önemli parçası olan insan faktörünün göz ardı edildiği ve sosyal mühendislik saldırıları konusunda yeterli bilinç seviyesinin olmadığı,
5. Kurumlarda kullanılan antivirüs yazılımlarının güncel tutulmadığı,
6. Siber güvenlik çalışmalarının en önemli personeli denebilecek sistem yöneticilerinin güvenlik konusunda yeterli deneyime sahip olmadıkları,
7. Bir siber olayın meydana gelmesi durumunda olması gereken kurum içi koordinasyonun yetersiz olduğu,
8. Sistemlere ve hizmetlere erişim ve kontrol politikasının olmadığı,
9. Sistemler tasarlanırken güvenlik boyutunun yeteri kadar önemsenmediği,
10. Kablosuz ağların güvenliğinin yeteri kadar sağlanmadığı ve bu nedenle sistemlerin tehditlerin sömürüsüne açık olduğu,
11. İş sürekliliği planının olmadığı,
12. Yapılan port tarama saldırısının algılanmadığı,
13. DDoS saldırılarının olumsuz sonuçlar doğurduğu,
14. Kurumsal internet sayfalarında açıklıkların bulunduğu ve
15. Günlük kayıtlarının etkin ve verimli bir şekilde analiz edilemediği

bulgularına ulaşılmıştır (BTK-TÜBİTAK, 2011).

4.3.6 BOME 2008 ve USGT-2011 değerlendirmesi

2008 ve 2011 yıllarında yapılan siber güvenlik tatbikatlarına bakıldığında;

- BOME 2008 tatbikatına 8 kamu kurumu katılmış iken düzenleyicileri arasında BTK'nın da yer aldığı USGT-2011'e 42 kurum ve kuruluş katılım sağlamıştır.
- İlk defa USGT-2011'de isteyen kurum ve kuruluşlara gerçek saldırılar gerçekleştirilmiştir.
- BOME 2008 ve USGT-2011'den elde edilen bulgular karşılaştırıldığında:
    - Saldırı tespit sistemlerinin etkin bir şekilde kullanılamaması,
    - Sistemlerin ürettiği günlük kayıtlarının analiz edilememesi,
    - Önceden belirlenmiş bir bilgi güvenliği yönetim politikasının olmadığı veya olaylara bu politikaya göre müdahale edilmediği ve

- Siber olay meydana geldiği sırada kurum içi koordinasyonun sağlanamadığı

konusunda ortak tespitlerin yapıldığı görülmektedir. Dolayısıyla 2008 yılındaki tatbikatta yapılan ve yukarıda bahsedilen bazı tespitlerin USGT-2011'de de yapılmış olması, aradan geçen 3 yıllık süre içerisinde söz konusu tespitlerde bahsedilen sorunların çözümüne yönelik yeterli ve etkin bir çalışmanın yapılmadığı izlenimi uyandırmaktadır.

Bununla birlikte, USGT-2011'in katılımcı sayısının oldukça fazla olması, katılımcılar arasında BTK tarafından düzenlenen ve denetlenen elektronik haberleşme sektörünün ve siber ortamın büyük aktörlerinin yer alması, BTK'nın bu alanda yapılacak çalışmalara öncülük edebileceğini ortaya koymaktadır.

Özetlemek gerekirse, BİT'lerin yaygınlaşması, bu yaygınlaşma ile birlikte kötücül faaliyetlerin de artması diğer ülkelerle birlikte ülkemizde de meydana gelen gelişmeler arasında yer almaktadır. Bununla birlikte, siber güvenliği sağlama çalışmaları yürüten ülkelerde genellikle, ulusal bir siber güvenlik politikasının olduğu, bu politikanın bir parçası olarak U-STİM yapılarının kurulduğu, bu yapıların görevlerinin ve siber suçlarla mücadelenin çerçevesini belirleyen hukuki düzenlemelerin yapıldığı, kamu-özel sektör işbirliğinin tesis edilmeye çalışıldığı gözlemlenmektedir.

Ülkemizdeki duruma bakıldığında ise, ulusal bir siber güvenlik politikasının bulunmaması, siber tehditlerle ve olaylarla mücadele edecek ulusal seviyede bir yapı olmakla birlikte bu yapının hukuki dayanaktan yoksun olması ve etkin bir rol alamaması, siber tehditlerle mücadele konusunda kamu-özel işbirliğinin tesis edilememiş olması siber güvenliğin sağlanması yönündeki çalışmalara yeterli önemin verilmediği izlenimi uyandırmaktadır.

SONUÇ VE ÖNERİLER

Kullanıcıları, kuruluşları hatta ülkeleri hedef alan siber tehditler giderek karmaşık bir yapıya sahip olmakta, siber âlemin fiziki sınırları ortadan kaldırmasıyla dünyanın farklı coğrafyalarında yaşayan siber suçlular bir araya gelmekte, hedefli saldırılar ve organize suçlar artmaktadır.

Dünyada her saniye yüzlerce siber olayın meydana geldiği bir ortamda bir kuruluş için siber tehditlere karşı gerekli önlemlerin alınması, siber olaylara hızlı ve etkin bir karşılık verilmesi, hem saldırının hedefi olan organizasyon için hem de müşterileri için kritik bir önem arz etmektedir. Tehdidin veya olayın fark edilmesi, analiz edilmesi ve gerekli önlemlerin alınması ne kadar hızlı ve dikkatli yapılırsa, oluşabilecek hasarlar, kurtarma maliyetleri ve benzer olayların gelecekte tekrar yaşanması ihtimali o ölçüde azalacaktır. Dolayısıyla kullanıcılara güvenli bir siber ortam sunmada, oluşabilecek siber tehditlere ve olaylara hızlı ve etkin bir şekilde müdahale edebilme yeteneğine sahip olmak önemli bir gereksinimdir. Bu gereksinimi ulusal seviyede karşılayabilecek etkin çözümlerden biri U-STİM yapısıdır.

Sadece kamu, sadece özel veya kamu-özel işbirliği öncülüğünde yapılanabilen U-STİM, siber tehditler ve olaylarla mücadelede müşterilerine karşı belirli bir sorumluluğu olan, siber olayları ele almak için gerekli hizmetleri sunan ve siber olaylardan sonra hizmet verdiği müşterilerine geri kurtarma süreçlerinde destek veren bir hizmet organizasyonudur.

Siber tehditlerle mücadele konusunda Gerek ITU tarafından hazırlanan GCA'da gerekse AB tarafından hazırlanan ADA'da, sayıları ve karmaşıklığı giderek artan siber tehditlerle mücadele amacıyla;

- Ulusal siber güvenlik stratejisinin oluşturulması,
- Siber olayların yönetimini sağlayacak yapıların (U-STİM) kurulması,
- Kamu-özel sektör arasındaki işbirliğinin tesis edilmesi ve
- Uluslararası işbirliklerinin kurulması

teşvik edilmekte ve bu çalışmaların ulusal düzeyde yürütülmesinin daha etkin ve verimli olacağı değerlendirilmektedir.

Bu çerçevede siber güvenliğin sağlanması evrensel küme olarak kabul edilecek olursa,

- Ulusal siber güvenlik stratejisini (USGS),
- Siber güvenlik mevzuat altyapısını ve
- U-STİM yapısını

bu evrensel kümenin birer alt kümesi olarak değerlendirmek mümkündür.

U-STİM yapısı, ancak bir siber güvenlik stratejisinin ve siber güvenlik mevzuatının mevcudiyeti durumunda etkin olabilmektedir. Diğer bir anlatımla, siber güvenliğin sağlanması faaliyetinin amacına ulaşabilmesi için konuya ilişkin bir stratejiye, hukuksal düzenlemelere ve siber olaylara ulusal seviyede müdahale edecek bir yapıya ihtiyaç olduğu sonucuna ulaşılmaktadır. Bu kapsamda, ülkemizde U-STİM yapısının başarılı olabilmesi için öncelikle söz konusu büyük resmin birer parçası olan;

- USGS'nin belirlenmesi ve
- Siber güvenliğe ilişkin hukukî düzenlemelerin yapılması

konularında çalışmalar yapılması gerekmektedir.

a. Ulusal siber güvenlik stratejisinin hazırlanması

Maruz kalınan siber tehditlerin ve saldırıların farkında olunması ve bunların tespit edilmesi, bu tehdit ve saldırıların yol açabileceği maddi manevi zararların öngörülmesi ve bütün bunların akabinde alınması gereken önlemlerin makro seviyede belirlenmesi, USGS oluşturma sürecinde yapılabilecek çalışmalar arasında yer almaktadır. Ulusal siber güvenlik bir ülkedeki tüm tarafları ilgilendiren bir konu olması dolayısıyla, söz konusu stratejinin hazırlanmasında ulusal seviyede bir işbirliğinin sağlanmasına özen gösterilmelidir. Bu doğrultuda ülkemizde USGS hazırlamak için yapılacak çalışmalarda USGS'nin:

- **Usûl olarak;**
  - Başbakanlığın koordinatörlüğünde tüm Bakanlıkların, kamu kurumlarının merkez teşkilatlarının, kolluk kuvvetlerinin, yargı birimlerinin, akademik çevrelerin, sivil toplum kuruluşlarının ve elektronik haberleşme sektörü temsilcilerinin katılımı ile hazırlanması,
- **İçerik olarak;**
  - Taraflar arasındaki görev ve sorumluluklara yer vermesi,
  - Kamu kurumlarının ve özel sektör kuruluşlarının kendi bünyelerinde STİM yapılarını oluşturmalarına ilişkin hususları içermesi,
  - U-STİM yapısının kurulmasına ilişkin yönlendirmelerde bulunması,
  - Ulusal ve uluslararası işbirliğini teşvik etmesi,
  - Kamu-özel sektör işbirliğini arttırıcı hükümleri içermesi,
  - Siber güvenlik konusundaki farkındalığı arttırma çalışmalarına ilişkin detayları barındırması,

gerektiği değerlendirilmektedir.

b. Siber güvenlik konusunda hukukî düzenlemelerin yapılması

Ülkemizde Bilgi Toplumu Stratejisi Eylem Planının 88 numaralı Eylemi ile TR-BOME kurulmuştur. Ancak TR-BOME'nin idarî, mali ve operasyonel yapısının, faaliyet alanının hukuki dayanaktan yoksun olması nedeniyle anılan yapının siber tehditlerle ve olaylarla mücadelede yeteri kadar etkin ve verimli olamadığı değerlendirilmektedir. Ayrıca konuya ilişkin uluslararası kuruluşların tavsiyeleri ve ülke uygulamaları incelendiğinde, çoğunluk itibarı ile ulusal siber güvenlik stratejisinin olduğu, söz konusu stratejiye dayanan U-STİM'e ve siber tehditlerle mücadele eden diğer kurum ve kuruluşlara esnek ve güçlü bir faaliyet ortamı sunan bir siber güvenlik mevzuatının bulunduğu gözlemlenmektedir. Bu bağlamda ülkemizde BTK'nın öncülüğünde:

- Siber güvenliğin sağlanmasını,
- U-STİM (UST@M) yapısının kurulmasını, yapısını, sunacağı hizmetleri, hizmet vereceği kurum ve kuruluşları, faaliyet alanını, sorumluluklarını ve

- UST@M ile kolluk kuvvetleri ve adli birimler arasındaki işbirliğini düzenleyen hukuki çerçevenin oluşturulması gerektiği değerlendirilmektedir.

Bu konuda yapılacak hukuki düzenlemelerin; siber ortamın sınır aşan yapısını dikkate alarak siber olaylarda UST@M'ın iletişime geçeceği ihtisas sahibi kolluk kuvvetlerinin belirlenmesi, tüm ülke çapında yetkili özel savcıların görevlendirilmesine imkân vermesi, siber tehditlerle mücadelenin kendine özgü niteliklerini göz önünde bulundurması, siber olayların tespiti halinde gecikmeksizin müdahale edilerek delillerin toplanmasını mümkün kılan hükümleri içermesi yerinde olacaktır. Bu sayede, siber tehditlerle ve suçlarla mücadelede esnek ve etkin bir ortam sağlanacaktır.

Mevzuatın, UST@M'ın faaliyet alanını ve özellikle mali, idari ve operasyonel yapısını olabildiğince esnek bir şekilde belirlemesine, UST@M'ın ilgili kolluk birimleri ve yargı mercileri ile etkin bir iletişim sağlayacak ve işbirliğini artıracak hükümler içermesine özen gösterilmelidir. Çünkü siber ortam, sınır aşan ve dinamik yapısı gereği esnek bir alan olduğundan, bu alanda mücadele edecek birimlerin de en az bu ortam kadar esnek bir yapıya sahip olması gerektiği değerlendirilmektedir.

Son olarak, yapılacak hukuki düzenlemelerde TR-BOME'nin AR-GE amaçlı bir STİM olarak hizmet verebilmesi için gerekli düzenlemelerin yapılmasının, böylece TR-BOME'nin hukuki bir zemine kavuşturulmasının faydalı olacağı mülahaza edilmektedir.

c. UST@M Yapısı

Siber tehditlerle ulusal seviyede mücadelede en önemli yapı olan UST@M'ın, siber güvenlikle ilgili ulusal tüm tarafları kapsayacak şekilde öncülük yapma gücüne sahip olan devletin öncülüğünde kurulması ve idare edilmesi halinde daha etkin ve verimli olacaktır.

Türkiye'de UST@M yapısının aşağıda sıralanan özelliklere sahip olması gerektiği değerlendirilmektedir. Bu çerçevede;

- Siber güvenlik konusunda çalışmalar yürüten kurum olarak BTK, siber güvenlik konusunun tarafları olan erişim sağlayıcılar, mobil haberleşme hizmeti sunan işletmeciler ve kamu kurumları ile koordinasyon sağlayarak etkin bir UST@M yapısının kurulması çalışmalarına öncülük etmelidir.
- BTK'nın öncülüğünde siber güvenliğin tüm taraflarının birlikte çalışması ile ulusal siber güvenliğin sağlanmasının en önemli adımlarından biri olan UST@M yapısının kurulmasına ve işletilmesine yönelik hukuki düzenlemeler yapılmalıdır.
- Ülkemizde UST@M çalışmalarının kamu-özel işbirliği şeklinde yürütülmesi kurulacak yapının etkin ve verimli olmasına önemli katkılar sağlayacaktır.
- Cumhurbaşkanlığı, Türkiye Büyük Millet Meclisi (TBMM), Başbakanlık, bakanlıklar, tüm kamu kurumlarının merkez teşkilatları, büyükşehir ve il belediyeleri ile özel sektör kuruluşları bünyesinde STİM yapılarının kurulması teşvik edilmeli, bu yapının kurulması kamu kurumlarına, yerel yönetimlere ve özel sektör kuruluşlarına kademeli olarak zorunlu hale getirilmelidir.
- UST@M yapılarının genellikle merkezi olması, personel sayılarının çok fazla olmaması nedeniyle müşterilerine olaylara yerinde müdahale desteği sunamadıkları, bunun yerine çoğunlukla olay koordinasyon hizmeti sundukları görülmektedir. Bu nedenle kamu kurumlarında yaşanacak siber olaylara yerinde müdahale edilebilmesini sağlamak amacıyla Devlet-STİM yapısının oluşturulması yararlı olacaktır.
- Genelde siber güvenlik özelde ise STİM alanında araştırmalar yapacak, siber tehditlere müdahalede kullanılacak araçların ve çözüm önerilerinin geliştirilmesine katkıda bulunacak AR-GE amaçlı bir STİM'in kurulmasının yararlı olacağı değerlendirilmektedir. Bu bağlamda TR-BOME'nin STİM alanında AR-GE çalışmaları yürütecek ve ülkemizde bu konudaki AR-GE faaliyetlerinin koordinatörlüğünü üstlenecek bir yapıya dönüştürülmesi yararlı olacaktır. Ayrıca kurulacak UST@M'ın söz konusu AR-GE merkezi ile işbirliği içinde çalışması sağlanmalıdır.

- Kurulacak UST@M'ın kamu kurumlarına, özel sektöre ve sivil toplum kuruluşlarına, yerel yönetimlere ve vatandaşlara hizmet verecek şekilde yapılandırılması uygun olacaktır.
- UST@M, 7/24 çalışanları olan ayrı bir organizasyon şeklinde yapılandırılmalıdır.
- UST@M yapısının yönetim kurulunda, kendi STİM yapılarını kurmuş olan kamu kurumlarının yanı sıra, özel sektör kuruluşlarının ve sivil toplum örgütlerinin birer temsilcilerinin dönüşümlü olarak yer almaları sağlanmalıdır. UST@M'ın yönetim kurulunun, başkanlığını BTK'nın yürüteceği, iki üye kamu kurumları arasından, iki üye özel sektörden, iki üye belediyelerden, iki üye üniversitelerden ve iki üye sivil toplum örgütleri arasından olmak üzere toplamda 11 üyeden oluşacak şekilde yapılandırılmasının uygun olacağı değerlendirilmektedir (Şekil Ek-1.1). Üyelerin görev süreleri 2 yıl ile sınırlandırılmalıdır.
- Siber olaylara ve tehditlere müdahale politikasının oluşturulması ve bu politikaya dayanan siber olaylara karşı koyma süreçlerinin tanımlanması UST@M'ın etkinliğini artıracaktır.
- UST@M'ların, en az bir uluslararası platforma üye oldukları, bu platformlarda aktif bir şekilde görev aldıkları, söz konusu işbirliği tecrübesinin UST@M tarafından geliştirilen araçlara yansıdığı göz önünde bulundurularak ülkemizde kurulacak olan UST@M'ın uluslararası platformlara katılım sağlamasını teminen, yapılacak ulusal ve uluslararası işbirliği ve bilgi paylaşımı faaliyetlerine ilişkin politika ve süreçler belirlenmelidir.
- UST@M'ın yapılandırılmasında sunulacak hizmetlerin belirlenmesi önem arz etmektedir. Bu doğrultuda UST@M'ın asgari olarak;
    - Reaktif hizmetler kapsamında
        - Alarm ve uyarılar
        - Güvenlik olaylarının ele alınması
            - Olaya müdahale koordinasyonu
        - Güvenlik açıklıklarının ele alınması
            - Açıklığa karşı koyma koordinasyonu
    - Proaktif hizmetler kapsamında
        - Duyurular

- Güvenlik kalite yönetimi hizmetleri kapsamında ise
  - Farkındalık oluşturma ve
  - Güvenlik danışmanlığı yapma özellikle güvenlik politikası geliştirme

hizmetlerini sunabilecek şekilde yapılandırılması uygun olacaktır.

- Siber âlemin doğasından kaynaklanan dinamik ve esnek yapısı dikkate alınarak UST@M'ın personel yapısının dinamik olması ve ilk aşamada asgari hizmetleri sunabilecek uygun niteliklere sahip 15-20 personelin 7/24 çalışmak üzere istihdam edilmesi başarılı bir başlangıç sağlayacaktır.
- UST@M'ın bağımsız bir bütçeye sahip olması, yürüteceği faaliyetlerde esnek davranabilme imkânı sağlayacaktır. Bu amaçla UST@M'dan hizmet alacak kurum ve kuruluşların ödeyecekleri yıllık aidatlar ve UST@M'ın üstleneceği projelerden elde edeceği gelirlerin, söz konusu bütçenin oluşturulmasında kullanılabileceği değerlendirilmektedir.

KAYNAKLAR

5651, 2007, 4 Mayıs 2007 Tarihli ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

ALBERTS Chris vd., 2004, Defining Incident Management Processes for CSIRTs: A Work in Progress, Carnegie Mellon, CMU/SEI-2004-TR-015

ALBERTS Christopher, DOROFEE Audrey, 2005, OCTAVE Threat Profiles

APCERT, 2009, Annual Report

ARBOR NETWORKS, 2007, Worldwide Infrastructure Security Report

ARBOR NETWORKS, 2009, Worldwide Infrastructure Security Report

AUSCERT, 2011, http://www.auscert.org.au (25.03.2011)

AVG, 2010, http://www.avg.com.au/news/avg_turkey_and_russia_the_worlds_riskiest_web_surfers/, (13.07.2011)

BAKIRCI Yasin, 2010, İfade Hürriyeti Bağlamında İnternet İçerik Düzenlemeleri Ve Uygulamaları

BOTFREI, 2011, https://www.botfrei.de/tr/

BROWN Moira J. West vd., 2003, Handbook for Computer Security Incident Response Teams (CSIRTs), CMU/SEI-2003-HB-002

BTK, 2011, Basın Açıklaması (10.06.2011)

BTK-TÜBİTAK, 2011, Ulusal Siber Güvenlik Tatbikatı 2011 Sonuç Raporu, Yayımlanmamış Rapor

BUGÜN, 2011, http://www.bugun.com.tr/haber-detay/158686-secim-gunu-buyuk-operasyon-haberi.aspx

CCC, 2011, https://www.ccc.go.jp/en_index.html

CISCO, 2010, Annual Security Report, Highlighting global security threats and trends

CNCERT/CC, 2008, Annual Report

CNCERT/CC, 2011, http://www.cert.org.cn/english_web/index.htm, (30.03.2011)

CSA, 2011, https://cloudsecurityalliance.org

DEMİR Ömer Oğuzhan, KÜÇÜKUYSAL Bahadır, 2011, Sınıraşan Organize Suçlar

DHS, 2009, National InfrastructureProtection Plan

DPT, 2006, Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)

EC, 2010, A Digital Agenda for Europe, http://ec.europa.eu/information_society/digital-agenda/index_en.htm

EHK, 2008, 10 Kasım 2008 tarih ve 27050 sayılı Resmi Gazete yayımlanan Elektronik Haberleşme Kanunu

ENISA, 2006a, A Step-By-Step Approach On How To Set Up A CSIRT, Deliverable WP2006/5.1(CERT-D1/D2)

ENISA, 2006b, CERT cooperation and its further facilitation by relevant stakeholders, Deliverable WP2006/5.1(CERT-D3)

ENISA, 2007, A basic collection of good practices for running a CSIRT, Deliverable WP2007/2.4.9/1 (CERT-D3.1)

ENISA, 2010, Baseline Capabilities of National / Governmental CERTs Part 2: Policy Recommendations, Version 1.0 (initial draft)

ENISA, 2011, http://www.enisa.europa.eu, (12.04.2011)

FIRST, 2011, http://www.first.org, (24.03.2011)

FORWARD, 2010, Managing Emerging Threats in ICT Infrastructures, Deliverable D3.1: White book: Emerging ICT threats

GELBSTEIN Eduardo, KAMAL Ahmad, 2002, Information Insecurity, ITU

GTISC, 2011, Emerging Cyber Threats Report, Georgia Tech Information Security Center

GOVCERT.NL, 2009, Annual Review

GOVCERT.NL, 2010 Operational Framework

GOVCERT.NL, 2011, http://www.govcert.nl/english/home

HOLLANDA, 2011, The National Cyber Security Strategy (NCSS)

HOWARD John D., LONGSTAFF Thomas A., 1998, A Common Language for Computer Security Incidents

IBM, 2010, Cyber defense: Understanding and combating the threat

IMPACT, 2011, http://www.impact-alliance.org/home/index.html, (12.07.2011)

ITU, 2007a, Global Cybersecurity Agenda

ITU, 2007b, World Information Society Report Beyond WSIS

ITU, 2009, Cybersecurity: The Role and Responsibilities of an Effective Regulator

ITU, 2010, GSR 2010 Discussion Paper, The role of ICT regulation in addressing offenses in cyberspace

KILLCRECE vd., 2003a, Organizational Models for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon, CMU/SEI-2003-HB-001

KILLCRECE vd., 2003b, State of the Practice of Computer Security Incident Response Teams (CSIRTs)

KOM, 2011, Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı 2010 Raporu

MASERA Marcelo vd., 2011, ICT aspects of power systems and their security

MCAFEE, 2011, Threats Report: First Quarter 2011

MICROSOFT, 2010, Security Intelligence Report, Volume 9

MICROSOFT, 2011, Security Intelligence Report, Volume 10

NORTHCUTT Stephen, 2003, Computer Security Incident Handling, SANS

PWC, 2011, Getting real about cyber threats: where are you headed?

RESMİ GAZETE, 2011, 15 Temmuz 2011 Tarihli ve 27995 Sayılı Resmî Gazete

SCARFONE Karen vd., 2008, Computer Security Incident Handling Guide, National Institute of Standards and Technology, ABD

SILICKI Krzysztof, MAJ Mirosław, 2008, Barriers to CSIRTs cooperation Challenge in practice the CLOSER Project

SOPHOS, 2010, Security Threat Report

SOPHOS, 2011, Security Threat Report Mid-Year 2011

ŞEN Bilal, 05.05.2011, Sözlü Görüşme, Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Bilişim Suçlarıyla Mücadele Şube Müdürü, Emniyet Amiri

TR-BOME, 2011, http://www.bilgiguvenligi.gov.tr/cert/index.php (13.07.2011)

TÜBİTAK-UEKAE, 2008, BOME 2008 Bilgi Sistemleri Güvenliği Tatbikatı Tatbikat Sonuç Raporu

TÜBİTAK-UEKAE, 2009, Türkiye Bilgisayar Olayları Müdahale Ekibi Faaliyet Raporu 2007 – 2008

TÜİK, 2010a, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması Sonuçları

TÜİK, 2010b, Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması

TÜİK, 2011, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması

ULAKBİM, 2011a,

http://www.ulakbim.gov.tr/hakkimizda/tarihce/ulaknet/dunbugun.uhtml

ULAKBİM, 2011b, http://www.ulakbim.gov.tr/ulaknet/calistay/09/Didim_Calistayi-OLTA_Sistemi.pdf

Ulak-CSIRT, 2011, http://csirt.ulakbim.gov.tr/

US-CERT, 2008, Quarterly Trends And Analysis Report, Volume 3

US-CERT, 2009, Quarterly Trends And Analysis Report, Volume 4

US-CERT, 2011, http://www.us-cert.gov, (29.03.2011)

WIIK Johannes, KOSSAKOWSKI Dr.Klaus-Peter, Dynamics of Incident Response

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

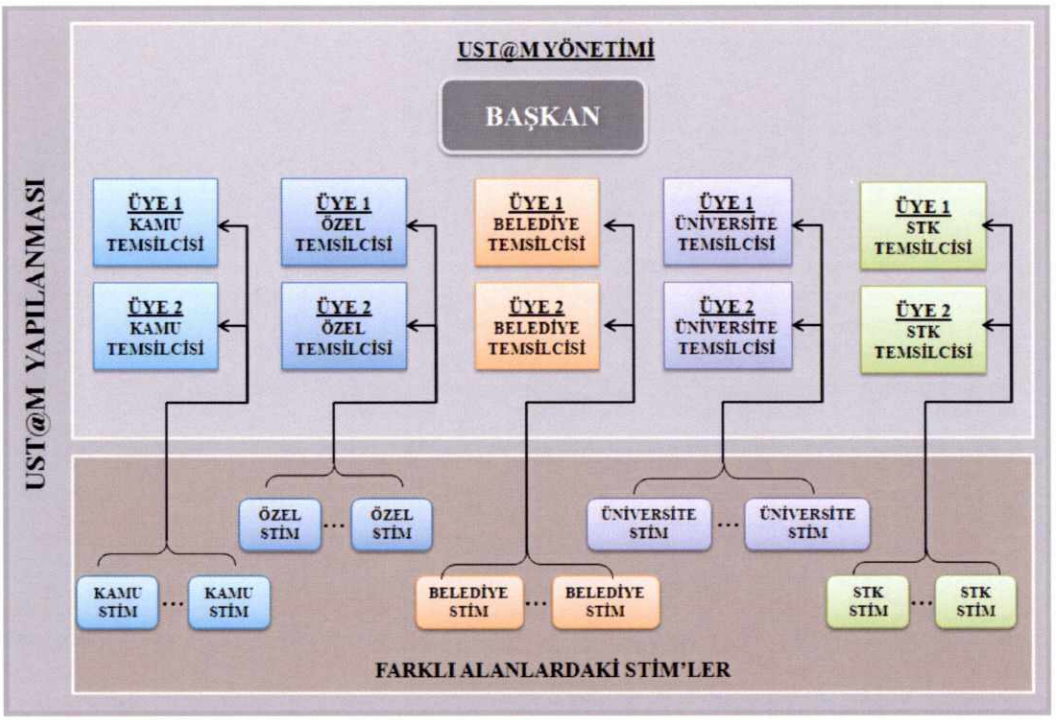
Yüksel GÜNAYDIN

ÖZGEÇMİŞ

1978 yılında Elazığ'da doğdu. İlk, orta ve lise öğrenimini Elazığ'da tamamladı. 2002 yılında Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. 2003 yılında Türk Telekomünikasyon A.Ş.'de Telekom Uzman Yardımcısı olarak çalışmaya başladı ve 2 yıldan fazla bu görevi yaptıktan sonra 21 Haziran 2008 tarihinde Bilgi Teknolojileri ve İletişim Kurumu'nda (eski adıyla Telekomünikasyon Kurumu) Bilişim Uzman Yardımcısı (eski adıyla Telekomünikasyon Uzman Yardımcısı) olarak göreve başladı. Halen Bilgi Teknolojileri ve İletişim Kurumu Bilgi Teknolojileri Dairesi'nde çalışmaktadır. Evli ve bir çocuk babasıdır.

Ek

Şekil Ek.1


UST@M YAPILANMASI
UST@M YÖNETİMİ
BAŞKAN
ÜYE 1 KAMU TEMSİLCİSİ
ÜYE 2 KAMU TEMSİLCİSİ
ÜYE 1 ÖZEL TEMSİLCİSİ
ÜYE 2 ÖZEL TEMSİLCİSİ
ÜYE 1 BELEDİYE TEMSİLCİSİ
ÜYE 2 BELEDİYE TEMSİLCİSİ
ÜYE 1 ÜNİVERSİTE TEMSİLCİSİ
ÜYE 2 ÜNİVERSİTE TEMSİLCİSİ
ÜYE 1 STK TEMSİLCİSİ
ÜYE 2 STK TEMSİLCİSİ
KAMU STİM
KAMU STİM
ÖZEL STİM
ÖZEL STİM
BELEDİYE STİM
BELEDİYE STİM
ÜNİVERSİTE STİM
ÜNİVERSİTE STİM
STK STİM
STK STİM
FARKLI ALANLARDAKİ STİM'LER