
GAZİ ÜNİVERSİTESİ
Gazi
1926

ORGANİZASYONLAR ARASI SİBER TEHDİT BİLGİ PAYLAŞIMI DEĞERLENDİRMELER VE ÖNERİLER

Ali Melih KANCA

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2021

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ali Melih KANCA

08/06/2021

ORGANİZASYONLAR ARASI SİBER TEHDİT BİLGİ PAYLAŞIMI DEĞERLENDİRMELER VE ÖNERİLER

(Yüksek Lisans Tezi)

Ali Melih KANCA

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2021

ÖZET

Siber uzaydaki varlıkları hedef alan saldırılar, tehditler veya ihlaller, organizasyonların karşılaştığı zorlukların başında gelmektedir. Bu zorlukların aşılabilmesi, siber tehditlerin tespit edilmesi ve önlenmesi için bu tehditler hakkında bilgilere ihtiyaç vardır. Siber tehditlerin paylaşımı konusunda işbirliği, olası tehditlerle mücadelede büyük öneme sahiptir. Bu tez çalışmasında; ülkemizde siber tehdit bilgisi paylaşımına ilişkin gerçekleştirilen çalışmalar incelenmiş, ülkemizde siber tehdit bilgisi paylaşım çalışmalarının artırılması, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberindeki işbirliği çalışmalarının genişletilmesi ve Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planında yer alan bilgi paylaşım çalışmalarının artırılması gerektiği değerlendirilmiştir. Ayrıca tehdit bilgisi paylaşımına ilişkin ABD, AB ve İngiltere'de olmak üzere en yaygın kullanılan dünya yaklaşımları incelenmiş, ülkemizde siber tehditlere dair güncel bilgilerin gerçek zamanlı olarak paylaşılması amacıyla organizasyonlar (kurumlar, birimler veya şirketler) arasında bir işbirliği platformunun oluşturulması önerilmiştir. Ayrıca organizasyonların gelişmiş siber tehditleri önleyebilmesi için siber tehdit bilgilerine duyulan ihtiyaçların belirlenebilmesi ve bünyelerindeki eksikliklerin giderilebilmesi amacıyla Zack Bilgi Boşluğu (ZBB) modelinden faydalanılmış ve analizler yapılmıştır. Organizasyonların gelişmiş siber tehditleri önlemede faydalanabilecekleri hususları belirlemek için ise Maslow'un İhtiyaçlar Hiyerarşisinden (MİH) yararlanılarak öneriler ve işbirliği platformu geliştirilmiştir. Ayrıca ZBB ve MİH analizleri ile siber tehdit bilgisine yönelik bakış açısının geliştirilmesine katkı sağlanmıştır. Sonuç olarak; bu tez kapsamında incelenen ve sonuçta siber tehdit bilgi paylaşımı konusunda organizasyonlar için önerilen işbirliği modeli ile paydaşlar arasında deneyimlerin paylaşılabileceği bir ekosistem oluşturulabilecek, siber tehditlerle topyekûn mücadele edilmesi kolaylaşacak ve en önemlisi bu alanda yapılacak olan Ar-Ge çalışmalarının kapsamının geliştirilmesi ile daha kapsamlı ürünlerin geliştirilmesi sağlanabilecektir. Bu tez kapsamında önerilen hususlar ile siber güvenlik kapasite ve yetenek geliştirilmesinde daha kapsamlı çalışmalar yapılabilecek, potansiyel ve yeni tehditler kapsamlı olarak araştırılabilecek, gelişmiş tehditleri engelleyebilecek ürünlerin geliştirilmesine katkı sağlanabilecek ve sonuçta siber vatanın savunulmasına katkılar sağlanabilecektir.

Bilim Kodu : 92403
Anahtar Kelimeler : Siber tehdit bilgisi, istihbaratı, ittifakı ve paylaşımı, Maslow'un İhtiyaçlar Hiyerarşisi, Zack Bilgi Boşluğu, analiz, öneri, model
Sayfa Adedi : 105
Danışman : Prof. Dr. Şeref SAĞIROĞLU

CYBER THREAT INFORMATION SHARING BETWEEN ORGANIZATIONS EVALUATIONS AND SUGGESTIONS

(M. Sc. Thesis)

Ali Melih KANCA

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2021

ABSTRACT

Cyber attacks, threats or breaches targeting entities in cyberspace are among the main challenges faced by organizations. Information about cyber threats is needed to overcome these difficulties and to detect and prevent these threats. Cooperation in sharing the cyber threats is great importance in combating possible threats. In this thesis; the studies on cyber threat information sharing in our country were examined. It was evaluated that the cyber threat information sharing activities of our country's institutions should be increased, the cooperation and collaboration activities should be improved, expanded and included not only in the guidelines but also included in the national strategies and action plans. In addition, the most widely used world approaches to sharing threat information, the USA, the EU and UK were examined. As a result, it was suggested that a collaboration platform for organisations (institutions, units or companies) should be developed and cyber threat information or intelligence (CTI) is shared in this platform among those in real time. In addition, the Zack Knowledge Gap (ZKG) model was used for analyzing and determining the needs of CTIs in order for organizations to prevent advanced cyber threats and eliminating the deficiencies in their structures. By making use of Maslow's Hierarchy of Needs (MHN), recommendations and suggestions based on CTIs were made to determine the points that organizations or countries can benefit in preventing advanced cyber threats. Moreover, new models were proposed, new analysis were made, and evaluatoins and suggestions were presented. It can be concluded that the results of ZKG and MHN analyses might help to improve our perceptions and perspective to CTIs. As a result; with the cooperation model, which is examined within the scope of this thesis and proposed to be created in our country on CTI sharing, an ecosystem where stakeholders can share experiences and threats will be created, and it will be easier to combat cyber threats collectively and securely. It will be also possible to develop better products, strategies, plans, defence mechanisms, and R&D studies against cyber attacks more than before. With the issues proposed within the scope of this thesis, cyber security capacity and skill development can be increased, potential threats can be investigated comprehensively and handled easily, better prevention and protection can be achieved for advanced threats in homelands.

Science Code : 92403

Key Words : Cyber threat information, alliance and sharing, Maslow's Needs Hierarchy, Zack Knowledge Gap, analysis, suggestion, model

Page Number : 105

Supervisor : Prof. Dr. Şeref SAĞIROĞLU

TEŞEKKÜR

Çalışmalarım süresince tez danışmanlığımı üstlenerek bana yol gösteren, tecrübeleri ile beni yönlendiren, çalışmanın yürütülmesinde katkı ve destek sunan danışmanım Prof. Dr. Şeref SAĞIROĞLU'na, kıymetli destekleri ile her zaman yanımda olan çok değerli aile üyelerime ve arkadaşlarıma teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
APT	Gelişmiş Kalıcı Tehditler (Advanced Persistent Threat)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
C2	Komuta & Kontrol (Command & Control)
CERT	Computer Emergency Response Team
CERT.FI	Finland Computer Emergency Response Team
CERT.EE	Estonian Computer Emergency Response Team
CIF	Collective Intelligence Framework
CIS	Center for Internet Security
CISCP	Cyber Information Sharing & Collaboration Program
CISP	Cyber Information Sharing Program
CRIT	Collaborative Research Into Threats
CSIRT	Computer Emergency Response Team
CTA	Siber Tehdit İttifakı (Cyber Threat Alliance)
CTI	Cyber Threat Information
CTX	Cyber Threat XChange
DDoS	Hizmet Reddi Saldırıları (Denial-of-Service Attack)
DHS	United States Department of Homeland Security
ECS	Enhanced Cybersecurity Services
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response Teams
FS-ISAC	Financial Services Information Sharing & Analysis Center
IoT	Nesnelerin İnterneti (Internet of Things)
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ITU	International Telecommunication Union

Kısaltmalar	Açıklamalar
ITU-IMPACT	ITU Multilateral Partnership Against Cyber Threats
MHN	Maslow's Hierarchy of Needs
MISP	Malware Information Sharing Platform
MITM	Ortadaki Adam Saldırısı (Man-In-The-Middle)
MİH	Maslow'un İhtiyaçlar Hiyerarşisi
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity Communications Integration Center
OTX	Açık Tehdit Değişimi (Open Threat Exchange)
PPP	Kamu Özel Ortaklığı (Public Private Partnership)
SCADA	Merkezi Denetim ve Veri Toplama
SİP SOME	SOME İletişim Platformu
SOME	Siber Olaylara Müdahale Ekibi
STIX	Structured Threat Intelligence eXpression
STB	Siber Tehdit Bilgisi
TAXII	Trusted Automated Exchange of Indicator Information
TI	Güvenilir Tanıtıcılar (Trusted Introducers)
TIP	Threat Intelligence Platform
TTP	Tactics Techniques & Procedures
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USOM	Ulusal Siber Olaylara Müdahale Merkezi
ZBB	Zack Bilgi Boşluğu
ZKG	Zack Knowledge Gap

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin ve internetin son yıllarda büyük bir hızla gelişme göstermesi ile birlikte bu teknolojiler hayatımızda önemli bir yer edinmekte ve yaşamımızın bir parçası haline gelmektedir. Kurum/kuruluşlar ve organizasyonlar ise gelişen teknolojiye kayıtsız kalmamakta, sundukları hizmetleri siber ortama taşımakta ve bilişim teknolojileri vasıtasıyla faaliyetlerini gerçekleştirmektedir. Söz konusu bilişim teknolojileri, kuruluşların yanı sıra elektrik, su ve haberleşme gibi hayatın devamlılığının sağlanmasında çok önemli paya sahip olan kritik altyapı sektörlerinde de yaygın bir şekilde kullanılmaktadır. Buna bağlı olarak, sunulan hizmetlerin ve kritik altyapı sistemlerinin bilişim teknolojilerine bağımlı hale gelmesi ile birlikte dijital verinin kullanımı ve dijital veri hacmi de artmaktadır.

Teknolojideki gelişmeler, internet kullanım oranı ve dijital verinin hacmi arttıkça, siber alandaki güvenlik riskleri artmakta ve bu riskler giderek küreselleşmektedir. Akıllı telefonlara, Nesnelerin İnternetini oluşturan internete bağlı cihazlara ve bilgisayar sistemlerine yönelik artan bağımlılık nedeniyle siber güvenlik kavramı ise giderek önem kazanmaktadır. Kritik bilişim altyapılarını ve sistemlerini hedef alan siber tehditler, ülkeler ve kuruluşlar için en büyük zorluklardan biri haline gelmiştir. Siber güvenliğin sağlanması ve kritik bilişim altyapılarının korunması, ülkelerin güvenliğinin ve ekonomik refahının sağlanmasında çok önemli bir role sahiptir. Ayrıca organizasyonların gerçekleştirdikleri faaliyetlerin devamlılığının sağlanması ve itibarının korunması açısından önem arz etmektedir. Böylesine gelişen ve büyüyen siber tehditlere karşı daha güçlü tedbirlerin alınması gerekmekte, ülkelerin ve kuruluşların ise bu tehditlere yönelik kapasitelerini güçlendirmesi gerekmektedir. Bu çerçevede, ana vatanımızın bir parçası olarak algılamamız gereken “ülke verilerimizin veya varlıklarımızın”, ülkemize ait bilişim sistemlerinin, altyapılarının ve tüm kurum ve kuruluşlar ile vatandaşlarımıza ait varlıkların, kısaca Siber Vatanın korunması ve güvenliğinin sağlanması önem arz etmektedir.

Siber uzaydaki varlıkların, altyapıların, sistemlerin ve verilerin gizliliğinin ve güvenliğinin sağlanması amacıyla çeşitli tedbirler alınmaktadır. Bu tedbirlerin alınabilmesi ve doğru becerilerin uygulanabilmesi için ise siber tehditler hakkında bilgi sahibi olunması gerekmektedir. Olası saldırıların gerçekleşmeden önlenebilmesi amacıyla siber tehditlerin

tanınması, etkilediği sistemlerin belirlenmesi ve bu tehditlerin olası etkileri hakkında bilgi edinilmesi gerekmektedir. Bu kapsamda, siber tehditlere yönelik doğru tedbirlerin uygulanabilmesi amacıyla siber tehditler ve tehdit aktörleri hakkında bilgi edinilmesine imkân tanıyan siber tehdit bilgilerine ihtiyaç duyulmaktadır.

Bunun yanı sıra, siber uzaydaki tehdit yelpazesi giderek genişlemekte, yeni saldırı aktörleri ve yöntemleri ortaya çıkmaktadır. Bu tehditlere yönelik güvenlik tedbirlerinin alınması için tehditlere dair en güncel bilgilerin hızlı bir şekilde elde edilmesi gerekmektedir. Bunun yanında, siber tehditlere yönelik bilgilerin tek bir kaynaktan elde edilebilmesi mümkün olamamakta, organizasyonlar diğer paydaşların bilgi ve birikimlerine ihtiyaç duymaktadır. Gelişen tehdit ortamı ve tehdit bilgilerine duyulan ihtiyacın artması siber güvenlik çalışmalarının önemli bir bileşeni olan bilgi paylaşımı ve işbirliğinin önemini daha da artırmaktadır.

Bu kapsamda, Siber Vatanın topyekûn savunulabilmesi, siber tehditlerle daha etkin mücadele edilebilmesi amacıyla organizasyonlardaki siber tehdit bilgisi kapasitesi ile yeteneklerin geliştirilebilmesi ve beslenen kaynakların zenginleştirilmesi için siber güvenlik ekosisteminin oluşturulması ve siber tehditlere karşı elde edilen bilgi, deneyim ve tecrübenin diğer paydaşlarla paylaşılması gerekmektedir. Siber tehditlere dair bilgilerin diğer paydaşlarla paylaşılarak her paydaşın savunma kapasitesinin artırabileceği ve Türkiye'de siber güvenlik alanında dayanıklılığın güçlendirilebileceği değerlendirilmektedir. Bu bağlamda bu tez çalışmasında, Türkiye'de siber tehdit bilgisi yönetimi ile tüm aktörlerin paylaşıma değer katacağı işbirliğinin siber tehditleri önlemede önemli rol oynayacağı savunulmuştur.

Bu çalışmada, Türkiye'de siber tehdit bilgisi paylaşımı konusunda gerçekleştirilen çalışmalar analiz edilmiş, tehdit bilgisi paylaşımında dünya genelinde kullanılan modeller araştırılarak en yaygın modeller incelenmiştir. Diğer ülkelerde de benzer bilgi paylaşım modelleri bulunmakla birlikte, hazırlanan bu yüksek lisans tezinde en yaygın kullanılan ve işlevselliği ile ön plana çıkan paylaşım modelleri çalışma kapsamına dâhil edilmiştir.

Çalışma kapsamında ülke örnekleri de incelenerek, organizasyonlar arasında tehdit bilgisi paylaşımının geliştirilmesi gerektiği değerlendirilmiş ve Türkiye'de organizasyonlar

arasında siber tehdit bilgisi paylaşım platformlarının oluşturulmasına dair kavramsal çerçeve ortaya konulmuştur.

Bu çerçevede bu tez çalışması kapsamında;

- Siber tehdit bilgisinin tanımı ve türleri, tehdit bilgilerinin siber güvenliğin sağlanmasına yönelik katkıları, tehdit bilgisi paylaşımında kullanılan modeller, standartlar ve protokoller üzerine dünyada gerçekleştirilen çalışmalar hakkında fikir sahibi olunabilmesi amacıyla literatür taraması gerçekleştirilmiştir.
- Siber tehdit bilgi paylaşımında en yaygın kullanılan ve Avrupa Birliği (AB) ve Amerika Birleşik Devletleri (ABD)'nde yer alan 3 model incelenmiştir. AB ve ABD'de konu kapsamında yayımlanmış kaynak çeşitliliğinin daha fazla olması, diğer ülkelere kıyasla tehdit bilgilerinin paylaşımı konusunda gerçekleştirilen çalışmaların yer aldığı doküman ve raporlara daha fazla erişim imkânı olması sebebiyle AB ve ABD'de yer alan modeller çalışma kapsamında değerlendirilmiştir.
- Zack Bilgi Boşluğu ve Maslow'un İhtiyaçlar Hiyerarşisi analizinden faydalanılarak ülkemizde tehdit bilgisi paylaşımına yönelik gerçekleştirilen çalışmalar incelenmiştir. Bu çerçevede, Türkiye'de tehdit bilgilerinin paylaşımı konusunda yapılan çalışmalar, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ile Rehberi ve ülkemizde şu ana kadar yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları incelenmiş, Türkiye'de işbirliğinin geliştirilmesine yönelik öneriler sunulmuştur.
- Ayrıca organizasyonların gelişmiş siber tehditleri önleyebilmesi için gerçekleştirmesi gereken çalışmaların belirlenebilmesi ve bu konudaki eksikliklerin giderilebilmesi amacıyla öneriler sunulmuştur.
- Organizasyonların tehdit bilgisi paylaşımı konusunda bünyelerindeki eksikliklerin belirlenmesi için Zack Bilgi Boşluğu analizi gerçekleştirilmiştir. Bu yöntem çerçevesinde, organizasyonların bünyelerindeki stratejik boşluklar belirlenmiş ve bu boşlukların doldurulmasına yönelik öneriler belirtilmiştir.
- Organizasyonların gelişmiş siber tehditleri önleyebilmesi amacıyla gerçekleştirmesi gereken çalışmalar üzerine Maslow'un İhtiyaçlar Hiyerarşisinden faydalanılmıştır. Bu kapsamda, organizasyonların bilinen siber saldırıların yanı sıra siber uzaydaki gelişmiş siber saldırıları da engelleyebilecek yeteneğe sahip olmasının gerektiği değerlendirilmiş, organizasyonların mevcut siber tehdit bilgilerini zenginleştirmesi ve

bu bilgileri diğer paydaşlarla paylaşarak kapasitesini artırması gerektiği değerlendirilmiştir. Bu sayede, yapay zekâ ve Gelişmiş Kalıcı Tehditler (APT) temelli gelişmiş tehditleri tespit edebilme yeteneğine sahip olunabileceği değerlendirilmiştir.

Bununla birlikte, siber tehdit bilgisi, türleri ve paylaşımına ilişkin dünyada gerçekleştirilen çalışmalar hakkında bilgi sahibi olunabilmesi amacıyla literatürdeki çalışmalar incelenmiştir. Literatürde genel itibarıyla; siber saldırganların daha inovatif ve gelişmiş yöntemler kullanmaya başlaması ile siber tehditlerin tespitinin ve engellenmesinin daha zor hale geldiği ve tehdit bilgilerinin ise siber tehditlerin engellenmesinde organizasyonlara büyük katkı sağladığı belirtilerek siber tehdit bilgi paylaşım modelleri, bilgi paylaşımı için kullanılan standartlar ve protokollere yer verilmiştir. Ayrıca siber tehdit bilgi paylaşım ekosistemine katılım sağlanmasının sağlayacağı avantajlardan bahsedilmektedir. Literatür çalışması sonucunda elde edilen bilgiler özetle aşağıda sunulmuştur:

- Thomas ve arkadaşları tarafından 2018 yılında gerçekleştirilen çalışmada [1], siber saldırıların artışını engellemek için yeni yöntemler geliştirilmesi gerektiği belirtilerek, siber tehdit bilgisinin faydaları ve oluşturabileceği riskler, siber tehdit bilgisinin otomotize bir şekilde işlenmesinin ortaya koyduğu zorluklar, siber tehdit bilgisi paylaşımında insan rolü, kültürel ve dilsel zorluklar, eyleme geçirilebilir siber tehdit bilgisi için tehdit bilgisinin barındırması gereken özellikler ve tehdit bilgisi paylaşımında kullanılan 3 yaygın paylaşım modeli incelenmiştir. Bu modeller, direkt bilgi paylaşımına imkân sunan "peer to peer", yayımlanan olayların paydaştan ortak havuza iletildiği "peer to repository" ve bu modellerin birleşiminden oluşan "hibrid" modelden oluşmaktadır.
- Jasper tarafından 2016 yılında yapılan diğer bir çalışmada [2] ise ABD Siber Tehdit Bilgisi Paylaşım Çerçeveleri, federal hükümet yapıları, gönüllü programlar ve siber tehdit bilgisi paylaşımında karşılaşılan zorluklar ele alınmıştır. ABD İç Güvenlik Bakanlığı (DHS) bünyesinde siber güvenliğe dâhil olan merkezi bir birim olarak hizmet veren Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezinde (NCCIC) siber güvenlik bilgilerinin analiz edildiği, zamanında ve eyleme geçirilebilir tehdit bilgilerinin paylaşıldığı ve müdahale, azaltma ve kurtarma çabalarının koordine edildiği belirtilmektedir. Ayrıca DHS'nin, çeşitli gönüllü bilgi paylaşım programları yürüttüğü Siber Bilgi Paylaşımı ve İşbirliği Programının (CISCP), federal hükümet ve

kritik altyapı sektörleri kuruluşları arasında siber tehdit, olay ve güvenlik açığı bilgilerini gerçek zamanlı olarak paylaştığı, bir diğer bilgi paylaşım programı Gelişmiş Siber Güvenlik Hizmetleri'nin ise ABD merkezli kamu ve özel kuruluşlara yönelik gelişmiş bir yaklaşımla koruma ve savunma sağladığı vurgulanmaktadır.

- Nenekazive ve Zubeida [3] ise konuyla ilgili olarak siber güvenlik ekipleri tarafından tehdit bilgilerinin paylaşım araçları ve standartları aracılığıyla paylaşıldığını, bu tehdit bilgisi paylaşım standartlarının uyumlu bir şekilde benimsenmesi ile siber güvenlik çalışmalarında büyük fayda sağlanacağını, ortak standartların benimsenmemesinin ise kuruluşlar ile sektör, ulusal ve uluslararası Bilgisayar Olaylarına Müdahale Ekipleri arasındaki siber tehditlerle ilgili etkili iletişimi zayıflatmaya neden olabileceğini raporlamıştır.
- Conti ve arkadaşları tarafından 2018 yılında yapılan çalışmada [4]; siber tehdit bilgisinin temel zorlukları ve sunduğu fırsatlar ele alınmıştır. Saldırganların daha inovatif ve akıllıca yöntemler kullanmaya başlaması ile birlikte saldırı yöntemlerindeki ilerlemelerin, saldırganın ve saldırının varış noktasının tanınmasını zor bir konu haline getirdiği, ayrıca siber suçluların zararlı kodlarında gelişmiş gizlenme yöntemleri kullanmasının genel güvenlik değerlendirme tekniklerini daha az verimli hale getirdiği vurgulanmıştır. Ayrıca gelişmiş siber saldırılara yönelik algılama, akıl yürütme, öğrenme ve hareket etme için yapay zekâ ve makine öğrenimi tekniklerinin uygulanması gerektiği vurgulanmış, güvenlik uygulayıcıları ve analistleri için güncel bilgiler sağlamak için bu yöntemlerin bir kombinasyonun gerekli olduğu belirtilmiştir.
- Abu ve arkadaşları tarafından 2018 yılında yapılan çalışmada [5]; hem organizasyonların hem de siber tehdit bilgisi sağlayıcılarının hangi bilgilerin siber tehdit bilgisi olarak kabul edildiğine dair tam bir anlayışa sahip olmadığı, bu nedenle siber tehdit bilgisini tanımlamak için daha fazla araştırmaya ihtiyaç duyulduğu belirtilmiştir. Bu çalışmada ayrıca tehdit bilgisi veri beslemeleri, tehdit bilgisi standartları ve tehdit bilgisi paylaşımında kullanılan araçları içeren mevcut siber tehdit bilgisi ürün ve hizmetleri de tanımlanmıştır. Bunun yanında, siber tehdit bilgisi paylaşımında karşılaşılan sorunlar ve zorluklar ele alınmıştır. Çalışmada ayrıca siber tehdit bilgisi potansiyelini tam olarak kullanmak için araştırma ve geliştirme çalışmalarının gerektiği, tehdit verilerini doğrulamak ve üyeler arasında paylaşılan tehdit verilerinin yeterli kalitede olmasını sağlamak için topluluk üyeleri arasında bir girişim bulunduğu, MITRE gibi bir araştırma ve geliştirme merkezinin tehdit paylaşan

paydaşlar arasındaki birlikte çalışabilirlik sorununu çözmek için tehdit bilgisi paylaşımı standartları (STIX, TAXII, CybOX gibi) geliştirdiği vurgulanmıştır.

- Murdoch ve Leaver tarafından 2015 yılında yapılan çalışmada [6] ise; İngiltere'deki şirketler ve devlet kurumlarının güvenli bir topluluk aracılığıyla yeni riskler ve güvenlik açıklıkları hakkındaki bilgileri paylaştığı bir işbirliği platformu olan Siber Güvenlik Bilgi Paylaşım Ortaklığı (CISP) incelenmiş, güven ve anonimlik ihtiyacını karşılamanın zorlukları ve bir siber güvenlik paylaşım girişimine katılmanın motive edici unsurları ele alınmıştır. Ayrıca siber güvenlik bilgilerini paylaşmaya motive eden üç ana faktörün ise; tehditlerin engellenmesine yönelik diğer paydaşlara yardımcı olunması, paydaşlar tarafından saygınlığın kabul edilmesi ve aynı sektörde faaliyet gösterenlerin ortak bir tehdide karşı savunmalarına yardımcı olunması olduğu belirtilmiştir.
- Vázquez ve arkadaşları tarafından 2012 yılında yapılan çalışmada [7], bilgi paylaşımını iyileştirmeye yönelik yaklaşımları belirlemek için siber savunma işbirliğinin dört yönü incelenmiştir. Bu hususlar; bilgi paylaşımına yönelik teşvikler ve engeller, işbirliğine dayalı risk yönetimi ve bilgi değeri algısı, veri alışverişinin geliştirilmesine yönelik prosedürel modellerin araştırılması ve siber savunma verileri için paylaşım mekanizmalarının otomatize edilmesi şeklinde sıralanmıştır. Çalışmada ayrıca siber savunma verilerinin paylaşımı için işbirliğine dayalı ilişkiler ve güvenilir ilişkiler kurma becerisinin gerektiği, ancak siber savunma işbirliğinin belirli zorluklar sunduğu, işbirliği platformları ile ilgili olarak net bir ortak anlayışa ulaşıldığında, veri paylaşımını iyileştirmeye yönelik prosedür modellerinin, bir kuruluşun risk modellerini bilgi paylaşım modelleriyle entegre etmesine yardımcı olacağı, tehdit seviyesi, öngörülen etki, risk metodolojisi ve risk yönetimi açısından karşılıklı yardımlaşmanın, işbirliği ağının etkinliğini artırmaya yardımcı olacağı belirtilmiştir.
- Liu ve arkadaşları tarafından 2019 yılında yapılan çalışmada ise [8]; siber tehdit bilgisinin paylaşıldığı ekosistem, bilgi paylaşımı için kullanılan standartlar, protokoller ve bilgi paylaşım modelleri incelenmiştir. Ayrıca siber tehdit bilgisinin ilk olarak 2013 yılında Gartner tarafından tanımlandığı ve tehdit bilgisinin organizasyonlardaki büyük miktardaki tehdit verilerinin işlenmesini kolaylaştırabildiği belirtilmiştir. Tehdit bilgisinin, tehditlerin savunulmasında pratik ve eyleme geçirilebilir, araştırılan ve yorumlanan bilgi olduğu ve saldırganın kimliği, saldırı yaklaşımları, önceden başlatılan saldırılar, saldırı hedefleri, hedeflenen sistemlerin güvenlik açıkları ve olası çözümler gibi birçok faktörü içerebileceği vurgulanmıştır.

Ayrıca genel olarak, tehdit bilgisi paylaşımı sürecinin üç modelle tanımlanabildiği, bunların ise; "Peer to peer, Eşler Arası", "Source-subscriber, Kaynak – Paydaş (Kaynaktan diğer paydaşlara bilgi akışı)" ve "Hub-and-spoke, Merkez – Paydaş (Paydaşlardan sağlanan tehdit bilgilerinin tüm paydaşlarla paylaşılması)" şeklinde sıralandığı vurgulanmıştır. Bunun yanı sıra, geleneksel tehdit bilgisi paylaşım yöntemleri çoğunlukla eşler arası ve kaynak-paydaş modellerine dayanırken, "merkez-paydaş" modelinin ise gelecek nesil tehdit bilgi paylaşım sistemlerinin geliştirilmesi için geniş çapta kabul gördüğü belirtilmiştir.

- Kokkonen ve arkadaşları tarafından 2016 yılında yapılan çalışmada [9]; risk düzeyine göre kuruluşlar arasında durumsal farkındalık bilgisinin paylaşılmasına yönelik model geliştirilmiştir. Bu model kullanılarak daha yüksek risk seviyelerine sahip doğrudan bağlantıların azaltılabildiği, daha güvenli bilgi paylaşım topluluklarının oluşturulabildiği vurgulanmıştır. Çalışmada ayrıca durumsal farkındalık bilgilerinin paylaşımının, kuruluşlar için son derece önemli olduğu, tehditlere karşı erken uyarı için gerekli olduğu, bununla birlikte paylaşılan bilgilerin kötüye kullanılma ihtimalinin bulunduğu ve bu tür bilgilerin paylaşılmasının riskli olabileceği belirtilmiştir.
- Win ve arkadaşları tarafından yapılan çalışmada [10], siber tehdit bilgisinin tanımı, siber tehdit bilgisi sağlayan bazı özel kuruluşlar ve siber tehdit bilgisi kullanımındaki bazı zorluklar incelenmiştir. Söz konusu çalışmada; operasyonel, taktik ve stratejik olmak üzere 3 farklı düzeyde siber tehdit bilgisi türünün bulunduğu belirtilmiştir. Ayrıca siber tehdit bilgisi kullanımında karşılaşılan zorluklar ise; tehdit verisinin aşırı yüklenmesi, tehdit verisi kalitesi, özel ve yasal sorunlar olarak sıralanmıştır.
- Mutemwa ve arkadaşları tarafından 2017 yılında yapılan çalışmada [11] ise; farklı paydaşların bağlamsal ve eyleme geçirilebilir siber tehdit bilgisini sorunsuz ve işbirliği içinde bir araya getirmesini, analiz etmesini ve zamanında paylaşmasını teşvik edebilecek ve etkinleştirebilecek kavramsal bir siber tehdit bilgisi paylaşım modeli ve platformunun oluşturulması ele alınmıştır. Ayrıca AlienVault, ThreatQ ve ThreatView tehdit bilgisi paylaşım platformları incelenmiştir. Çalışmada ayrıca tehdit bilgisinin paylaşımının stratejik, taktiksel ve operasyonel seviyelerde de gerçekleşebileceğinden, uygun bir paylaşım modelinin formüle edilmesi ve bunlar tarafından kabul edilmesinin önemli olduğu, bunun yanı sıra paydaşlar arasında paylaşılması gereken bilginin, çoğunlukla reaktif operasyonlarda yararlı olan bilgiden daha yüksek düzeyde olması gerektiği, ilgili tehdit bilgisinin bağlamsal ve eyleme geçirilebilir olması gerektiği ve

siber saldırılara ve siber suçlara karşı proaktif ve öngörücü yanıtlar sağlaması gerektiği belirtilmiştir.

- Zibak ve Simpson tarafından yapılan çalışmada [12]; paydaşların siber güvenlikle ilgili bilgi paylaşım faydaları ve risklerine yönelik tutumlarının keşfedilmesi hedeflenmiştir. Çalışmada; bilgi paylaşımı ile performans arasında bir bağlantı kuran deneysel verilerin eksik olduğu, tüm süreçler gibi bilgi paylaşımında da insan ve finansal kaynaklara ihtiyaç duyulduğu, sektörler arası siber güvenlik bilgilerinin üretimi, paylaşımı ve bu paylaşımı otomatikleştirmek için sistemlerin oluşturulması amacıyla daha fazla kaynak ayrıldığı ifade edilmiştir. Ayrıca bilgi paylaşımına yönelik deneysel desteğin yetersizliğinin iki önemli konuyu vurguladığı, birincisinin özel sektör kuruluşlarının rekabet, sorumluluk ve yatırım getirisi gibi çeşitli nedenlerden dolayı bilgi paylaşımına bazen ihtiyatlı davrandığı veya bilgi paylaşım çabalarına katılmaya isteksiz olduğu, ikincisinin ise bilgi paylaşım çabaları ve teknolojisi için değerlendirme yöntemlerinin olmamasının eksikliklerinin tespit edilmesini ve giderilmesini engellediği belirtilmiştir.

Sonuç olarak bu tez çalışmasında, bilgi paylaşımı ile ülkemizdeki siber güvenlik kapasitesinin ve direncinin artacağı değerlendirilmiş ve ulusal literatüre yeni bir bakış açısı kazandırılması hedeflenmiştir. Bu çerçevede, ABD'deki Siber Tehdit İttifakı'na benzer şekilde ülkemizde organizasyonlar arasında bilgi paylaşım platformunun oluşturulması önerilmiştir.

2. SİBER TEHDİT BİLGİSİ VE BİLGİ PAYLAŞIMI

Günümüzde bilgi teknolojilerinin kullanımı büyük bir hızla yaygınlaşmaktadır. Geleneksel iletişim yöntemlerinin yerini elektronik cihazlara, fiziksel nesnelerin ise yerini siber alandaki cihazlara bıraktığı siber uzayda birbirine bağlı cihaz sayısı, kullanıcı sayısı ve üretilen veri miktarı her geçen gün artmaktadır. Gelişen teknoloji ile birlikte siber uzayda ortaya çıkan tehditler de artmaktadır. Siber uzaydaki varlıkların korunabilmesi ve siber tehditlerle etkin bir şekilde mücadele edilebilmesi için siber tehdit bilgisine ihtiyaç duyulmakta, bu bilgilere sahip olunabilmesi için ise diğer paydaşlarla işbirliği yapılarak paydaşların bilgi birikiminden ve deneyimlerinden faydalanılması gerekmektedir.

2.1. Siber Uzay ve Siber Güvenlik

Son yıllarda yeni bir kavram olarak ortaya çıkan ve çok sayıda imkânı insanların kullanımına sunan siber uzay veya siber alan kavramı, internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan şeklinde tanımlanabilmektedir. Siber uzayın sunmuş olduğu kolaylıklar ve imkânlar siber uzayın sınırlarını her geçen gün artırmaktadır. Buna bağlı olarak siber uzayın sınırlarının genişlemesi ve bilişim teknolojilerinin kullanımının artması ile dijital veri hacmi de artmaktadır. Bununla birlikte, birçok kuruluşun sistemlerinin internete bağlı olması ve kritik servislerin bilişim sistemleri aracılığıyla sunulması, bu teknolojilerin getirmiş olduğu kolaylık ve imkânlarla birlikte yeni güvenlik tehditlerinin de ortaya çıkmasına neden olmaktadır. Ayrıca yeni teknolojilerin gelişmesi ve dijital veri hacminin artması ile dijital veriye yönelik tehditler de artmaktadır. Nitekim "son yılların önemli tartışma konularından biri olan dijital veri mahremiyeti konusu, önemini artırarak ve ulusal bir nitelik kazanarak dijital veri egemenliği söylemine evrilmeye başlamıştır. Dijital veriye başka aktörler tarafından müdahale edilebilmesi ise bu durumun ulusal güvenliğe yönelik tehdit algısını ortaya koymaktadır" [13]. Bu sebeple, bilişim sistemlerinin siber güvenliğinin sağlanması konusu son yıllarda oldukça önemli bir konu haline gelmiştir. Siber ortamın tehlikelerinin farkında olan ülkeler ise siber tehditleri önemli tehdit unsurlarından biri olarak kabul etmekte, bu konuya ulusal güvenlik stratejilerinde yer vermekte ve buna uygun siber güvenlik stratejileri ve politikalar geliştirmekte ve uygulamaktadır.

Siber güvenlik kavramı, “bütünlük, gizlilik ve erişilebilirlik prensipleri ışığında siber uzayda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar ve önlemleri, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünü” olarak ifade edilmektedir [14]. Uluslararası Telekomünikasyon Birliği (ITU) ise siber güvenliği; “kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü” şeklinde tanımlamaktadır [15]. Siber güvenlikte temel amaç bilgiyi korumak ve sistemlerin devamlılığını sağlamaktır. Siber saldırı ve olayların tespit edilerek engel olunması ve bilişim sistemlerinin saldırı/olay öncesi duruma döndürülmesi de siber güvenliğin amaç ve hedefleri arasında yer almaktadır.

Bilgisayar sistemlerini veya ağlarını bozmak veya işlevsiz hale getirmek için gerçekleştirilen faaliyetler olarak tanımlanabilen siber saldırılarda ise siber saldırganlar siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve altyapı sistemlerini hedef almaktadır. Böylelikle kamu bilişim sistemleri, kritik altyapı bilişim sistemleri hedef alınabilmekte, bilişim sistemleri üzerinden sunulan hizmetlerin aksamasına neden olunabilmektedir. Nitekim dünyada yaşanan bazı siber saldırılarda bunun örnekleri yaşanmıştır. 2007 yılında Estonya’daki kamu kuruluşlarına ait internet sitelerine ve bankacılık sistemine yönelik DDoS (Dağıtılmış Hizmet Reddi Saldırıları) saldırıları gerçekleştirilmiş ve bu sitelerin sunucuları hizmet veremez hale gelmiştir. 2008 yılında ise Gürcistan kamu internet siteleri DDoS saldırıları ile hedef alınmış ve bu siteler de belirli bir süre hizmet verememiştir.

2011 yılında İran’nın Natanz şehrindeki nükleer yakıt zenginleştirme tesisini hedef alan siber saldırıda ise “Stuxnet” adı verilen zararlı yazılım kullanılmıştır. Zararlı yazılımın hedefi enerji üretim ve dağıtımının kontrolü, su ve doğal gaz sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesinde kullanılan Denetleme Kontrol ve Veri Toplama Sistemi (Supervisory Control and Data Acquisition, SCADA) olup, saldırı sonucunda nükleer çalışmalar sekteye uğratılmıştır. 2015 yılında ise Ukrayna’nın Ivano-Frankivsk bölgesinde elektrik tesislerinin hedef alındığı ve 700 bin kişinin saatlerce elektriksiz kalmasına neden olan siber saldırı yaşanmıştır.

2017 yılında meydana gelen “WannaCry” saldırısında ise 99 ülkedeki 230 bin bilgisayar WannaCry fidye yazılımı ile hedef alınmıştır. Hedef alınan bilgisayardaki dosyalar şifrelenerek kullanıcılardan şifrenin çözülmesi karşılığında para talep edilmiştir. Saldırıdan İspanya'daki telekom şirketi Telefónica, enerji şirketi Iberdrola, İngiltere Ulusal Sağlık Servisi, Rusya İçişleri Bakanlığı, Rusya Acil Durum Bakanlığı gibi kuruluşlar etkilenmiş ve buradaki sistemler üzerinden sunulan hizmetlerde aksamalar yaşanmıştır. 2017 yılında “Notpetya” adı verilen bir fidye yazılımı ile Ukrayna başta olmak üzere dünya genelindeki pek çok bilgisayar hedef alınmıştır. Sonuç olarak, siber güvenliğin sağlanması konusu son yılların en önemli konularından biri haline gelmiştir. Bu kapsamda, özellikle son yıllarda bilişim sistemlerinin siber güvenliğini sağlamaya yönelik çeşitli önlemler alınmakta ve gerek maddi olarak gerekse insan gücü olmak üzere altyapı ve kapasiteyi artırıcı tedbirler alınmaya başlanmıştır [16].

Öte yandan, APT, DDoS saldırıları, botnet saldırıları, fidye yazılımları, oltalama saldırıları, Man-In-The-Middle (MITM) saldırıları, casus yazılım saldırıları, günümüzde siber saldırganlar tarafından yaygın kullanılan siber saldırı türleri olarak karşımıza çıkmaktadır.

APT saldırıları, yüksek düzeydeki sistemlerden bilgi elde edilmesi amacıyla gerçekleştirilen ve yaygın bilinen tekniklerin kombinasyonundan oluşan sofistike siber saldırı türleridir. APT saldırıları, belirli bir hedefe yönelik kalıcı saldırılar olup, birkaç adımda gerçekleştirilmektedir. APT saldırıları temel olarak casusluk ve veri hırsızlığı amacıyla gerçekleştirilmektedir. APT’lerin gelişmiş teknikler kullanması ve bilinmeyen güvenlik açıklıklarından yararlanması sebebiyle mevcut algılama yöntemleri için bir zorluk teşkil etmektedir. Bu bağlamda, APT saldırılarının tespiti edilmesi zor olabilmekte ve uzun sürebilmektedir. Bu saldırı türleri çok zor tespit edilebilmesi sebebiyle önemli hasarlara ve mali kayıplara neden olabilmektedir [17].

Banka veya çevrimiçi alışveriş sitesi gibi güvenilir bir aracıdan gelen iletilere benzeyecek şekilde tasarlanmış olan elektronik posta iletilerinin kullanımı ile kurbanların hedef alındığı saldırılar ise oltalama saldırıları olarak tanımlanmaktadır. Bu mesajlar ile genellikle kullanıcılardan hesap bilgilerini doğrulaması istenmekte ve kullanıcıyı tuzağa düşürebilmek amacıyla genellikle bir aciliyet duygusu barındıran ifadeler kullanılmaktadır. Hedef alınan kişiler bu mesajları güvenilir bir kaynaktan gelmiş şekilde algılamaktadır.

Oltalama saldırıları, insanların kullandığı sistemleri doğrudan hedeflemek yerine, sistemleri kullanan kişileri hedef almaktadır. Oltalama yöntemleri ile bilinçsiz kullanıcıları hedefleyerek büyük zararlara sebep olabilen oltalama saldırıları siber saldırganlar tarafından yaygın bir şekilde kullanılmaktadır.

DDoS saldırısı ise bir bilgi işlem veya bellek kaynağının çalışmasının engellenmesi amacıyla gerçekleştirilen ve bant genişliğinin tamamını kullanarak sistemin cevap vermesini engellemeyi hedefleyen siber saldırı türü olarak tanımlanabilmektedir. DDoS saldırısı ilk olarak Khan C. Smith tarafından 1998 yılında gerçekleştirilmiştir. Bu saldırı türünde hedef alınan sistemin çökertilmesi veya yavaşlatılması ile kullanılamaz hale getirilmesi amaçlanmaktadır. DDoS saldırıları, hedef sistemi kapasitesinden fazla dış iletişim isteklerine maruz bırakmakta ve sistem istek trafiğine cevap veremeyecek konuma gelmektedir. Bu saldırıların, servisin çökmesine sebep olanlar ve servisin aşırı yavaşlamasına neden olanlar şeklinde olmak üzere iki genel formu bulunmaktadır. Siber saldırganlar, ağ bağlantılı bir sistemin güvenlik açıklıklarını kullanmamakta, ancak kullanılabilirliğine karşı saldırılar gerçekleştirmektedir. 2007 yılında Estonya'da, 2008 yılında Gürcistan'da gerçekleştirilen siber saldırılar, DDoS saldırılarına örnek gösterilebilmektedir.

Kötü amaçlı botnetler, bir operatörün uzaktan yönetilmesi ile "Bot" adı verilen güvenliği ihlal edilmiş bilgisayarlardan oluşan bir ağdır. Botlar önceden tanımlanmış bazı işlevleri otomatik bir şekilde gerçekleştirmek için tasarlanmıştır. Botnet'ler, DDoS saldırıları, oltalama saldırıları ve kötü amaçlı yazılım yayma gibi birçok saldırıya imkân sağladığı için önemli ve büyüyen bir tehdit oluşturmaktadır.

Fidye yazılımı (Ransomware) saldırısı, hedef alınan bilgisayardaki verilerin şifrelenmesi veya bilgisayarın kilitlenmesi amacıyla kötü amaçlı kod kullanan bir kötü amaçlı yazılım türüdür. Siber saldırganlar, fidye yazılımı ile verileri kullanıcılar için erişilemez hale getirmekte ve dosyaların şifrelerinin çözülmesi için kullanıcıdan para talep etmektedir. 2017 yılında gerçekleştirilen "WannaCry" ve "NotPetya" saldırıları, bu saldırı türünde gerçekleştirilen saldırılar olarak gösterilebilmektedir. Fidye yazılımı ile kullanıcı ödeme yapmadığı sürece kullanıcının bilgisayarının devre dışı bırakılması amaçlanmıştır.

Casus yazılımlar, hedef alınan kişilerin bilgisayarlarına gizlice yüklenen kötü amaçlı kod sınıfı şeklinde tanımlanabilmektedir. Bu yazılımlar ile kullanıcıların davranışları sessizce izlenebilmekte, webde gezinme alışkanlıkları kaydedilebilmekte ve hedefin kullanıcı şifreleri elde edilebilmektedir.

MITM saldırısı ise ağda iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya veriler üzerinde değişikliğin yapılmasına imkân tanıyan bir saldırı yöntemi olarak tanımlanmaktadır. MITM saldırısı, taraflar arasında akan gerçek verileri ve verilerin kendisinin gizliliğini ve bütünlüğünü hedeflemektedir. MITM saldırılarında taraflar arasındaki iletişim kesilebilmekte veya yanıltıcı bir iletişim oluşturulabilmektedir.

2.2. Siber Tehdit Bilgisi

Siber tehditlerin çeşitliliği, sayıları ve niteliği arttıkça bu tehditlerin tespit edilmesi ve engellenmesi daha zor hale gelmektedir. Siber ortamın tehlikelerinin farkında olan organizasyonlar kurumsal siber güvenliğini korumaya yönelik çaba göstermekte, başta kritik altyapı sistemleri olmak üzere varlıklarını ve verilerini siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadır. Gelişen tehditlere karşı güvenlik stratejilerini sürekli olarak yenilemektedir.

Siber tehditler, bir veya daha fazla açıklığın sömürülmesi ile güvenlik önlemlerini aşabilecek, sistemlere yetkisiz erişimde bulunulabilecek, sistem yapısını bozarak kullanılamaz hale getirebilecek tehditler olarak tanımlanmaktadır [18]. Bir başka tanımda ise siber tehditler, birbirine bağlı ağlara yönelik tehditler olarak tanımlanmaktadır [19]. Diğer bir kaynakta ise; yetkisiz erişim sağlanması, tahribat oluşturulması, bilginin değiştirilmesi veya ifşa edilmesi faaliyetleri ile bilgi sistemleri üzerinden organizasyonel süreçlerini, varlıklarını, kişileri veya bir ulusu etkileyen potansiyel olaylar veya durumlar olarak tanımlanmaktadır [20].

Siber tehditlerin tespit edilmesi, sınıflandırılması ve gerekli tedbirlerin alınması, siber saldırıların önlenmesinde önemli bir rol oynamaktadır. Bununla birlikte, siber uzaydaki siber saldırıların özellikleri ve karmaşıklığı, güvenlik analistleri, olay müdahale ekipleri ve siber tehdit aktörleri arasında önemli bir mücadeleye sebep olmaktadır. Güvenlik analistleri ve olay müdahale ekipleri, savunma çabalarını gerçekleştirmeden önce siber

saldırıları tespit edebilmek amacıyla doğru becerilere ihtiyaç duymaktadır. Gerekli kontrollerin geliştirilmesi, kapsamlı bir tehdit analizi gerektirmektedir [21]. Bu çerçevede, organizasyonlar siber ortamdaki tehditlere yönelik varlıklarını korumak amacıyla siber tehdit bilgisine ihtiyaç duymaktadır. Çok sayıda saldırı ile başa çıkabilmek, saldırı özelliklerini derinlemesine incelemeden ve buna karşılık gelen akıllı savunma eylemlerini gerçekleştirmeden mümkün olamamaktadır. [3]

Siber tehdit bilgisi (STB) ise siber uzaydaki zararlı olayların azaltılmasına yardımcı olan bilgiler ve tehdit aktörleri hakkında bilgiler olarak tanımlanmaktadır. Siber tehditlerin tanımlanabilmesi ve bu tehditlerin tespit edilebilmesi için gerekli olan tehdit bilgisi ile siber saldırganların amaçları, motivasyonları, yöntem ve metotları hakkında bilgi sahibi olunabilmekte ve bu bilgiler organizasyonların tehdit risklerini belirlemesine yardımcı olmaktadır.

Siber tehdit bilgisi, toplanan verilerin analiz edilerek saldırganların düşüncelerini, amaçlarını, motivasyonlarını, yöntem ve metodlarını tespit etme amacı taşımaktadır. Siber saldırganlar tarafından kullanılan komuta kontrol sunucusuna ait IP adresi, oltalama saldırısında kullanılan e-posta veya bir zararlı aktivitede bulunan saldırgan ve saldırı tekniği hakkında bilgi siber tehdit bilgisine örnek olarak verilebilmektedir. Siber tehdit bilgisi; indikatörler, taktikler, teknikler ve prosedürler (TTPs), güvenlik uyarıları, tehdit bilgisi raporları ve araç konfigürasyonları bileşenlerinden oluşmaktadır [22].

Siber tehdit bilgisinin başlıca amacı, kurum ve kuruluşların tehdit risklerini tespit etmelerine yardımcı olmaktır. Bu saldırılara örnek olarak; sıfırıncı gün saldırıları, APT ve zararlı kod saldırıları örnek olarak gösterilebilmektedir. Bu tür saldırılar kurum ve kuruluşların sistemlerine ciddi zararlar verebilmektedir.

Siber tehdit bilgisinin kullanımı, bir organizasyonun güvenlik açıklıklarına odaklanarak, değerli bilişim varlıklarının korunmasını sağlamakta, aynı zamanda bir organizasyonun kötü niyetli bir aktörün her zaman bir adım önünde olmasına imkân tanımaktadır. Ayrıca bir organizasyonun sofistike saldırganların yapısını anlamasına ve sistemlerini daha iyi savunabilmek amacıyla bilinçli kararlar almasına olanak tanımaktadır. Hızlı hareket eden bir siber saldırıya karşı saldırı hakkında zaman kaybetmeksizin bilgi elde edilmesi saldırıların önlenmesinde önemli bir paya sahip olmaktadır.

Siber tehdit bilgisi, siber saldırganların teknik, taktik ve prosedürleri hakkında bilgi sunabilmekte, saldırganların oluşturdukları/oluşturabilecekleri tehditlere karşı ek bilgiler verebilmekte, alınması gerekli savunma mekanizmaları ve alınabilecek önlemler hakkında fikir verebilmektedir. Bu kapsamda, tehdit oluşturabilecek noktalara doğru çözüm önerilerinin sunulması, benzer ihlallerin gerçekleşmemesi adına alınacak önlemlerin daha bilinçli yapılandırılabilmesi mümkün olabilmektedir.

Organizasyonlarca siber tehdit bilgisinin etkin kullanımı ile yetenekli tehdit aktörleri belirlenebilmekte, siber tehdit ortamı hakkında güncel bilgiye sahip olunabilmektedir. Ayrıca bu bilgiler iç ve dış paydaşlarla paylaşılabilmektedir [23]. Siber güvenlik ekosistemi için çok önemli olan siber tehdit bilgisi ile olası veri kayıpları önlenebilmekte, güvenlik önlemleri yönlendirilebilmekte (Hackerlar tarafından kullanılan örüntüler tespit edilmekte ve gerekli önlemlerin alınmasına yardımcı olmakta) ve diğer paydaşlar bilgilendirilerek siber tehditlerle topyekûn mücadele edilebilmektedir.

Bunun yanında, siber saldırılarla mücadelede karşılaşılan bazı zorluklar bulunmaktadır. Bu zorluklardan biri ise siber suçlular tarafından istismar edilebilecek noktaların ve sistem açıklıklarının belirlenmesi gerektiğidir. Siber saldırganlar hedef aldıkları kurbanları aldatmak için yaygın yöntemlere ilave olarak son yıllarda daha akıllı ve aşina olunmayan yöntemleri tercih etmektedir [4]. Siber tehdit bilgisi ile olası siber saldırılarının tespit edilebilmesi, sistemlere yönelik zararlı girişimlerin izlenebilmesi, olası bir veri ihlalinin erken tespit edilmesi, ek ihlallerin tespit edilerek oluşabilecek zararların en aza indirgenmesi kolaylaşacaktır.

Bunun yanı sıra, gelecekteki ve mevcut saldırılar ile mücadele edebilmek ve bu saldırılara organizasyonları hazır hale getirebilmek amacıyla reaktif koruma yerine proaktif yaklaşım benimsenmesi bir zorunluluk haline gelmiştir. Mevcut siber güvenlik mekanizmaları genellikle reaktif niteliktedir. Etkin bir savunma sağlanabilmesi için siber güvenlikte reaktif yaklaşım yerine proaktif bir yaklaşım benimsenmesi gerekmektedir. Proaktif yaklaşım, potansiyel tehditlerin araştırılmasını ve bir güvenlik açığının istismar edilmeden önce bir çözüm uygulanmasını gerektirmektedir. Bu kapsamda ele alındığında, siber tehdit bilgisi ile beslenmiş bir proaktif yaklaşım güvenlik ekiplerine karar vermede yardımcı olabilecektir [24].

Bunun yanında, gelişmiş saldırıların belirlenebilmesi için yeni savunma yaklaşımlarının geliştirilmesi gerekmektedir. Saldırılar başlamadan önce tespit edilemese de tehditler önceden analiz edilebilmektedir. Siber tehdit bilgisi derin tehdit analizine yardımcı olabilmekte, aktif tehdit analizi yaklaşımları ile gelişmiş saldırı yöntemleri hakkında bilgi edinmeye yardımcı olmaktadır. Saldırganların davranışları siber tehdit bilgileri ile belirlenebilmekte ve siber güvenlik sistemleri özelleştirebilmektedir [8].

Ayrıca yapılan bazı araştırmalarda güvenlik uyarılarını takip etmenin oldukça zor olduğu, aynı zamanda bu araştırmada güvenlik ekipleri tarafından zararlı yazılım uyarılarına karşı harcanan zamanın büyük bir kısmının bilgi hatası nedeniyle harcandığı belirtilmektedir. Bu araştırmadan da anlaşıldığı üzere bilgi hatası kurumlara hem personel tedariki hem de bütçe yapılandırması açısından fazlasıyla zarar verebilmektedir. Bu problemleri çözmek veya azaltmak için de siber tehdit bilgisinin kullanımı önem teşkil etmektedir.

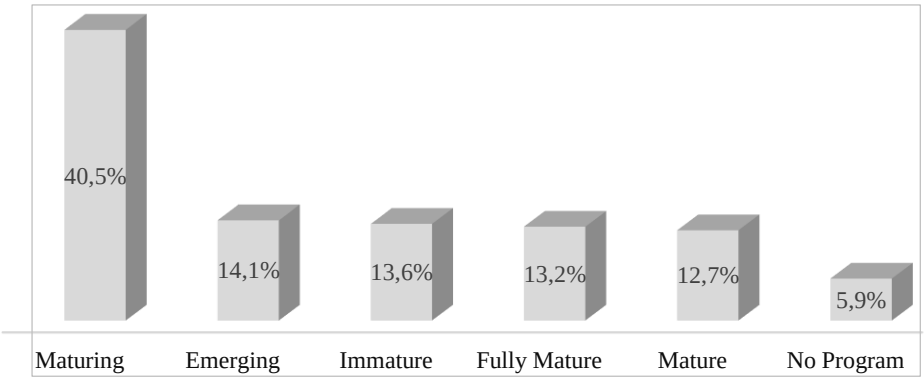
Sonuç olarak, siber tehdit bilgisi ile benzer ihlallerin gerçekleşmemesi adına alınacak önlemler daha bilinçli yapılandırılabilmekte, gerekli savunma mekanizmaları ve alınabilecek önlemler hakkında fikir edinilmekte, saldırganların teknik, taktik ve prosedürleri anlaşılabilmektedir. Tehdit oluşturabilecek noktalara doğru çözüm önerilerinin geliştirilmesi ve toplanan verilerin analiz edilerek, saldırganların oluşturdukları veya oluşturabilecekleri tehditlere karşı ek bilgiler elde edilmesi, hedeflenen saldırılara karşı kullanılan önlemlerin geliştirilmesine yardımcı olmaktadır.

Ayrıca siber tehdit bilgisi sayesinde; zararlı IP adresleri ve domainler ile zararlı girişimlerin izlenebilmesi, olası oltalama saldırılarının tespitinin kolaylaşması, verilerin toplanıp analiz edilmesi ve olası benzer durumlar için önlem alınması ve kurum üzerindeki zararının en aza indirgenmesi, veri kaybı veya sızıntısının hangi cihazlar üzerinde gerçekleştiği veya gerçekleşmekte olduğu bilgisinin elde edilmesi mümkün olabilmektedir. Siber tehdit bilgisinin organizasyonlara sağlayacağı avantajlar Çizelge 2.1.'de listelenmiştir.

Çizelge 2.1. Siber tehdit bilgisinin avantajları

Siber Tehdit Bilgisinin Avantajları
▪ Siber tehditlere ilişkin güncel bilgiye sahip olunabilmekte ▪ Siber tehditler ve tehdit aktörleri (Motivasyonlarını, yöntem ve metodları vb.) hakkında bilgi edinilmekte ▪ Tehdit riskleri belirlenebilmekte ▪ Hangi varlıkların risk barındırdığı belirlenebilmekte (Zafiyetler, güvenlik açıklıkları) ▪ Güvenlik önlemleri yönlendirilebilmekte ▪ Sistemlere yönelik zararlı girişimler izlenebilmekte ▪ Olası veri ihlallerinin erken tespit edilmesi sağlanabilmekte ▪ Proaktif yaklaşım benimsenebilmekte ▪ Yeni savunma yaklaşımları geliştirilebilmekte ▪ Personel ve bütçe, teknoloji harcamaları, emek ve zaman kaybı azaltabilmekte

Diğer taraftan, yapılan bir araştırmaya göre organizasyonların %5,9'nun siber tehdit bilgisine sahip olmadığı, bununla birlikte birçok organizasyonun kendi sistemlerini yetersiz bulduğu, yine organizasyonların %40,5'inin ise kendi siber tehdit bilgisi programlarını olgunlaştırdığı sonucu ortaya çıkmıştır. Şekil 2. 1.'de araştırmada yer alan organizasyonların siber tehdit bilgisi kapasitelerine ilişkin sayısal veriler belirtilmiştir.



Şekil 2.1. Organizasyonların siber tehdit bilgisi kapasitesi [25]

Tehditlerle ilgili bilgilere sahip olan organizasyonların daha bilinçli karar verebileceği değerlendirilmekte olup, organizasyonların siber tehdit bilgisi programlarında; zafiyetleri belirleyen, güvenliği destekleyen ve 7/24 izleyen bir sistemin olması, potansiyel sorunların

takip edilmesi için kara listeye alınmış web sitelerine ve kötü niyetli aktörlere yönelik verilerin bulunması gerekmektedir. Ayrıca saldırganların sistemlere nasıl girdiği, ne istediği, nasıl elde ettiğini ortaya koyan en son araştırmalara sahip olunması gerekmektedir [25]. Yapılan bir diğer çalışmada ise veri ihlallerin %80'inin siber tehdit bilgisi ile engellenebileceği ya da hasarının en aza indirebileceği sonucu ortaya çıkmıştır. Siber tehdit bilgisi çözümleri eyleme geçirilebilir çözümler olup, gerçek zamanlı önlemler alınabilmekte ve olası saldırılara karşı hazırlıklı olunabilmektedir.

Diğer taraftan, organizasyonlarda güvenlik ekipleri tarafından bilginin işlenmesi amacıyla taktiksel, operasyonel ve stratejik bilgi olmak üzere farklı bilgiler kullanılmaktadır. Taktiksel bilgi, olay müdahale prosedürleri için öneriler üzerine kurulmuştur ve kuruluşların güvenlik pozisyonlarını artırmada önemli bir rol oynamaktadır. Taktiksel bilgi, tehdit aktörleri tarafından kullanılan teknikler, taktikler ve prosedürlerle ilgili materyallerden oluşmaktadır.

Stratejik bilgi ise siber saldırı gruplarının ve saldırganların ortak belirli özelliklerine ilişkin bilgiler şeklinde tanımlanmaktadır. Stratejik bilgi, taktiksel bilgiden oluşturulan bilgi tabanı üzerine inşa edilmiş olup, güvenlik ekiplerinin önemli kararlar almalarına yardımcı olmak için kullanılabilmektedir. Stratejik bilgi, saldırının kaynağına yönelik aksiyon alınmasını sağlamaktadır. Stratejik tehdit bilgisi, üst düzey karar vericileri tehdit ortamı hakkında bilgilendirmek amacıyla kullanılmaktadır. Bu nedenle, stratejik bilgi ürünleri teknik terminoloji yerine iş riski konularına odaklanmaktadır.

Operasyonel bilgi ise siber saldırı belirtilerini hızlı, verimli ve zamanında tespit etmeyi amaçlamaktadır. Operasyonel bilgi genellikle bir kuruluşa karşı yapılması muhtemel operasyonların ayrıntılarıyla ilgili olup, bilinen saldırıların ayrıntılarının incelenmesiyle elde edilen bilgidir [26].

2.3. Siber Tehdit Bilgisinin Sahip Olması Gereken Özellikler

Siber tehdit bilgisi çözümünün benimsenmesi ve sürdürülmesi için minimum bazı gerekliliklerin bulunması gerekmektedir. Öncelikle siber tehdit bilgisi çözümlerinin kullanılabilmesi için plan, strateji ve insan ve teknoloji kaynağı gerekmektedir. SANS Enstitüsü tarafından yapılan ve şirketlerin tehdit bilgisini nasıl benimsediğini ve

kullandığını inceleyen bir ankette, ankete katılan şirketlerin %57'sinin siber tehdit bilgisinin entegrasyonu ve kullanımı için iyi tanımlanmış bir planın, organizasyonlar için en iyi uygulamayı temsil ettiğine inandıkları bildirilmiştir. Araştırmada ayrıca tehdit bilgisinin benimsenmesi ile ilgili boşlukların ve geçici çözümlerin tanımlanmasının önemli olduğu ve şirketlerin uygulama çabalarına rehberlik edecek uygun nitelikli uzmanlar bulmaya önem vermeleri gerektiği vurgulanmaktadır.

Bunun yanı sıra tehdit bilgisi çözümünün, mevcut güvenlik altyapısıyla sorunsuz bir şekilde bütünleşmesi ve tehdit bilgisi çözümünün tehdit bilgisinin alınması, analizi ve uygulanması ile ilişkili süreçlerin çoğunun otomatikleştirmesi gerekmektedir. SANS Enstitüsü'nün bir raporunda, algılama ve olay müdahale süreçlerini kolaylaştırmak için otomasyonun önemi vurgulanmaktadır. Raporda, otomasyonun güvenlik analistlerine önemli görevlere daha fazla zaman ayırmalarına imkân verdiği ve tehdit bilgisini operasyonelleştirmeyle ilgili idari yönlere daha az zaman ayırmalarına olanak tanıdığı belirtilmektedir. Raporda ayrıca otomasyonun tutarlılık sağlanmasına yardımcı olduğu ve aynı zamanda kalan süreç verimsizliklerinin ortadan kaldırılmasında yenilikçiliğin teşvik edildiği belirtilmektedir.

Bunun yanı sıra, siber tehdit bilgilerinin uygulanabilir olması için; güven, itibar, ilgi düzeyi, anonimlik, zamanlılık ve verilerin birlikte çalışabilirlik özelliklerini taşıması gerekmektedir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA); uygunluk, zamanlılık, doğruluk, bütünlük ve analiz edilebilirlik olmak üzere beş kriteri karşılayan uygulanabilir/eyleme geçirilebilir siber tehdit bilgisi tanımlamaktadır [27].

Uygunluk, bilginin içeriğinin ilgi düzeyini göstermekte olup, elde edilen tehdidin sistem için bir risk olarak tanımlandığını belirtmektedir. Bununla birlikte, uygunluk, eksiksizlik ve güven ile bir bütün olarak değerlendirilebilmektedir. Zira bilginin temin edildiği paydaş güvenilir değilse veya bilgi eksikse, söz konusu bilgi ilgili kabul edilmeyebilmektedir. Zamanlılık, güncel bilgileri zamanında paydaşlarla paylaşmak ve temin etmeyi ifade etmektedir. Bazı siber saldırılar saniyeler içinde gerçekleştirilebilmektedir. Hızlı bir bilgi paylaşım süreci, siber tehdit bilgisi paylaşımının önemli bir özelliğidir. Tehdit ortamı hızla değişmekte ve bu nedenle siber tehdit bilgisi hızlı bir şekilde değerlendirilmelidir. Bilgi paylaşımının hızlı bir şekilde gerçekleştirilmesinin önemi, bilginin değerinin çok kısa sürede yok olması halinde anlaşılabilmektedir. Bir paydaşın, bir e-posta içerisinde yer alan

bir kötü amaçlı bir bağlantı hakkında bir gösterge tespit etmesi halinde ve bu bilgiyi güvenilir bir platformda birkaç saniye içinde paylaşması halinde diğer paydaşlar tarafından tehdidin engellenerek riskin azaltılabilmesi mümkün olabilecektir.

Bunun yanı sıra, bir siber tehdit bilgisi paylaşım işbirliği oluşturmak, paydaşlar arasında kapsamlı bir güven ilişkisi gerektirmektedir. Güven konusu, siber tehdit bilgisi paylaşım ekosisteminde temel bir özellik olup, bilgi paylaşım ekosistemindeki en zor özellik olarak kabul edilmektedir [1]. ENISA tarafından, gizli verilere yetkisiz paydaşlarca erişim sağlanmaması, bilginin doğru kullanılması ve paylaşılan bilgilerin inandırıcı ve güvenilir olması olmak üzere üç güven ilişkisi belirlenmiştir. Ayrıca paydaşların, bir tehdit paylaşım topluluğunun güvenilir birer üyeleri olabilmesi için itibarlarını korumaları gerekmektedir. İtibar, yüksek kaliteli ve eyleme geçirilebilir siber tehdit bilgileri paylaşılarak ve siber tehdit paylaşım politikalarına uyarak zaman içinde oluşturulmaktadır. Güvenilirliği artırmak için, paydaşların sürekli olarak siber tehdit bilgisi paylaşması, çeşitli kaynakları ilişkilendirmesi ve paylaşılan bilgi ile ilgili olarak topluluğun sorularını yanıtlaması gerekmektedir [28].

Diğer taraftan, organizasyonlarda uygulanabilir olmayan tehdit göstergeleri nedeniyle, bir analist tarafından tüm verilerin değerlendirilmesi gerekebilmektedir. Bu nedenle, işbirliği ekosisteminde paydaşlar tarafından ölçeklenebilir bir uygunluk düzeyi filtresi kullanılması gerekmektedir. “Veri uygunluğu, veri kalitesinin önemli bir faktörüdür.” [29]. Paydaşların, envanterlerini bilerek sistemleri ile hangi siber tehdit bilgisinin ilgili olduğunu değerlendirmesi ve tanımlaması gerekmektedir.

Ayrıca organizasyonların, siber tehdit bilgisini yalnızca güvenilir paydaşlarla paylaşarak ve/veya içeriği anonimleştirerek paydaşların gizliliğine öncelik vermesi gerekmektedir. Anonim paylaşım, bir paydaşın henüz kendi sisteminin ihlal edildiğini açıklamak istemediği, ancak bilgiyi diğer paydaşlarla paylaşmak istediği durumlarda kullanılabilmektedir. Zira paydaşlar, itibarlarına zarar verebileceği korkusuyla ihlallerle ilgili bilgileri paylaşma konusunda isteksiz olabilmektedir [30].

Siber tehdit bilgisinin anonimleştirilmesi, güvenlik zafiyeti kapatılmadan önce kritik bilgilerin ortaya çıkmasını ve paydaşlara karşı kullanılmasını önleyebilmektedir. Anonimlik olmaması halinde, kötü niyetli paydaşlar tarafından kapatılmamış güvenlik

zafiyetleri, zafiyet barındıran paydaşlara yönelik kullanılabilmektedir. Siber tehdit bilgilerinin anonimleştirilmesi halinde kötü niyetli kişiler tarafından ele geçirilen verilerin çözümlenmesi zaman alacak ve bu zaman dilimi içerisinde paydaşlar söz konusu zafiyetlere yönelik gerekli tedbirleri alabilecektir. Anonimliğin sağlanması ile paydaşlar arasında paylaşılan bilgiler anonimleştirilecek ve böylece Ortadaki Adam (Man in the Middle) saldırılarına karşı söz konusu bilgiler korunabilecektir. Siber tehdit bilgisinin anonimliği içerik, meta veriler ve veri aktarımı dâhilinde oluşturulması gerekmektedir.

Bunun yanında, organizasyonlar siber tehdit bilgilerin paylaşmak istemekte ancak siber tehdit bilgisi paylaşımı için küresel olarak yaygın bir format bulunmamaktadır. Bu sebeple, paylaşılan veri formatlarının paydaşların sistemleriyle uyumlu olması gerekmekte ve tüm paydaşlar tarafından ortak bir format üzerinde anlaşmaya varılması gerekmektedir. 2014 yılında yapılan bir ENISA çalışmasına göre, topluluk tarafından benimsenen 53 farklı bilgi paylaşım standardı bulunmaktadır [1].

2.4. Siber Tehdit Bilgisi Paylaşımında Kullanılan Standartlar ve Platformlar

Siber tehdit bilgilerinin paylaşılması amacıyla birçok standart kullanılmaktadır. Bu standartların kullanılması ile tüm paydaşlar arasında aynı dilin konuşulması sağlanmakta, siber tehdit bilgisinin herkes tarafından anlaşılabilir ve kullanılabilir olması mümkün olmaktadır. Bu standartlara; Structured Threat Intelligence eXpression (STIX), Trusted Automated eXchange of Indicator Information (TAXII), Incident Object Description Exchange Format (IODEF), Collective Intelligence Framework (CIF) örnek verilebilmektedir [11].

Organizasyonların ve güvenlik uzmanının tehdit bilgisi verilerini toplama ve bu verilerin nasıl işleneceğini belirleme konusunda artan bir ilgisi bulunmaktadır. Ancak, tehdit bilgisi araçlarının yardımı olmadan bu tehdit verileri yönetilemez veri akışı haline gelebilmektedir. Bu nedenle, tehdit bilgisi paylaşımının yönetilmesine yardımcı olabilecek araçlar geliştirilmiştir.

Siber tehdit bilgisi paylaşımında, yetenekli, geniş kullanıma sahip olan ve MITRE tarafından geliştirilen STIX ve TAXII protokolleri bulunmaktadır. MITRE Corporation, siber tehdit bilgilerini standartlaştırılmış ve yapılandırılmış bir şekilde açıklamak ve

işbirliği yapmak için STIX ve TAXII standartlarını geliştirmiştir. Bugün itibariyle STIX, tehdit bilgisi verilerini tanımlamak için fiili standart olarak kabul edilmekte ve tehdit bilgisi paylaşım platformu tarafından yaygın olarak kullanılmaktadır. Ayrıca ENISA, AB üye devletleri için STIX/TAXII standartlarını tavsiye etmektedir [1].

STIX standardı, siber tehdit bilgisinin tanımlanması, elde edilmesi, karakterize edilmesi ve standardize edilmesi amacıyla geliştirilmiş olup, yapılandırılmış siber tehdit bilgilerinin tanımlanması, genişletilebilir, otomatikleştirilebilir ve güvenlik ekipleri tarafından okunabilir bir formatta temsil edilmesi için yapılandırılmış bir dildir. STIX, siber tehdit bilgisi konseptinin anlaşılabilmesi ve yönetebilmesi amacıyla oluşturulmuş bir standart olup, bilgisayar tabanlı saldırıların daha iyi anlaşılabilmesi, daha hızlı ve efektif bir şekilde yanıt üretilebilmesi adına kolaylık sağlamaktadır.

STIX yapılandırılmış tehdit bilgisine yönelik ortak bir mekanizma sağlamakta olup, gözlenebilir etkenler, indikatörler, siber olaylar, siber aktörlerin taktikleri, teknikleri ve prosedürleri (örüntü, zararlı yazılım, zararlı kod parçacıkları, siber ölüm zincirleri, araçlar, altyapılar ve hedefler vb.), istismar edilen hedefler (zafiyetler ve zayıflıklar vb.), eylem pratikleri (siber olaya yanıt verme veya zafiyet giderme), siber saldırı kampanyaları ve siber tehdit aktörleri bilgilerini içermektedir [31].

TAXII ise siber tehdit bilgilerinin platformlar arasında otomatik olarak paylaşılması için kullanılabilen ve MITRE tarafından geliştirilen bir standarttır. Temelde, kuruluşların yapılandırılmış siber tehdit bilgilerini güvenli ve otomatik bir şekilde paylaşmasına olanak tanımaktadır. TAXII, organizasyonların/kuruluşların ortaklarıyla bilgi paylaşmalarına yardımcı olmak amacıyla siber tehdit bilgisi alışverişi için bir dizi özellik olarak tanımlanmaktadır [32].

TAXII, organizasyonda eyleme geçirilebilir siber tehdit bilgilerinin paylaşılmasını sağlayan açık kaynaklı bir protokol ve hizmet belirtimidir. TAXII, güvenli ve otomatik bir şekilde sistemler arasında şifreleme, kimlik doğrulama, adresleme, uyarı ve sorgulama gibi yeteneklerle birlikte siber tehdit bilgi mesajlarının taşınması için ortak, açık spesifikasyonlar sağlayarak tehdit verilerinin hassasiyetini ele almaktadır.

Kuruluşlar arasında tehdit bilgilerinin paylaşımını sağlayan hizmetler ve mesaj alışverişi grupları TAXII standardında tanımlanmıştır ve bilgi üreticileri, tüketiciler ve geliştiriciler tarafından kullanılması amaçlanmıştır. Siber tehdit bilgilerinin birden çok paylaşım ortağı ve toplulukla otomatik olarak geniş bir şekilde paylaşma kabiliyeti TAXII tarafından mümkün kılınmaktadır. TAXII, otomatik bir paylaşım altyapısının parçası olabilecek hizmetleri ve mesaj alışverişlerini tanımlamakta ve aynı zamanda birden fazla paydaşla etkileşim kurmak amacıyla kullanılabilecek tek bir hizmet ve müşteri setini mümkün kılmaktadır. Bu sayede altyapı ve prosedürlere yeterli sayıda yatırım yapılmasını sağlamaktadır.

TAXII standardı ile siber savunma toplulukları içinde ve arasında tehdit bilgilerinin zamanında ve güvenli bir şekilde paylaşılması ve etkin siber tehdit bilgisi kümelerinin sağlam, güvenli ve yüksek hacimli bir şekilde alışverişi sağlanmaktadır [33]. Bu standart ile daha fazla kuruluşun tehdit bilgilerinin daha hızlı ve güvenli bir şekilde paylaşılması mümkün hale gelmektedir.

TAXII standardında; siber tehdit bilgi paylaşımı daha hızlı sağlanmakta, tanımlı hizmetler ve mesaj alışverişleri gibi büyük ölçüde manuel olarak yürütülen işler otomatize hale gelmekte, siber güvenlik alanında çalışan kişiler tehdit verilerini gerçek zamanlı olarak alabilmektedir. Ayrıca TAXII standardında tehdit paylaşım topluluklarına katılmanın önündeki teknik engeller azaltılarak daha fazla kuruluşun bu işleve katılması sağlanmaktadır.

Diğer taraftan, çeşitli siber tehdit bilgisi paylaşım standartları mevcut olmasına rağmen mevcut durumda organizasyonlar kurumsal, sektörel, ulusal ve uluslararası düzeylerde çalışan Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT) tarafından yaygın olarak benimsenen tek bir standart veya standartlar kümesi bulunmamaktadır. Bu durum, çeşitli kuruluşlar ve CSIRT ekipleri arasında iletişim açısından birlikte çalışabilirlik sorununu ortaya çıkarmaktadır. Ortak standartların benimsenmemesi, kuruluşlar ve kuruluşlar ile sektör, ulusal ve uluslararası CSIRT ekipleri arasındaki siber tehditlerle ilgili etkili iletişimi zayıflatmaya neden olabilmektedir.

Tehdit bilgisi paylaşım standartlarının uyumlu bir şekilde benimsenmesi, siber güvenlik çabaları için büyük fayda sağlayacaktır. CSIRT ekipleri tipik olarak STIX, TAXII ve

CybOX gibi siber tehdit bilgi paylaşım standartları ve protokollerine sahiptir. Johnson ve arkadaşlarına göre, standartlaştırılmış veri formatları ve taşıma protokolleri, otomasyonu etkinleştirdikleri ve kuruluşlar arasında makine hızında bilgi paylaşımına izin verdikleri için birlikte çalışabilirlik için önemli yapı taşlarıdır [3].

Tehdit Bilgisi Platformu (TIP) ise organizasyonların savunma eylemlerini desteklemek için gerçek zamanlı olarak birden fazla kaynaktan gelen tehdit verilerini bir araya getirmesine, ilişkilendirmesine ve analiz etmesine yardımcı olan yeni bir teknoloji disiplini olarak tanımlanmaktadır. Tehdit Bilgisi Platformları, çeşitli dâhili ve harici kaynaklar (sistem günlükleri ve tehdit bilgisi beslemeleri gibi) tarafından üretilen veri miktarını ele almak ve güvenlik ekiplerinin kuruluşlarıyla ilgili tehditleri tanımlamasına yardımcı olmak için geliştirilmiştir. Tehdit Bilgisi Platformları, birden çok kaynaktan ve formattan içe veri aktararak, bu verileri ilişkilendirerek ve ardından bir kuruluşun mevcut güvenlik sistemlerine aktararak, proaktif tehdit yönetimini otomatik hale getirmektedir [34].

Tehdit bilgisi platformları, tehdit aktörlerinin varlığını tespit ederek, saldırılarını engelleyip mücadele ederek veya altyapılarını bozarak kuruluşların saldırganlara karşı avantaj elde etmesini mümkün kılmaktadır. Tehdit bilgisi için taktiksel kullanım durumları arasında güvenlik planlama, izleme ve tespit, olay yanıtı, tehdit keşfi ve tehdit değerlendirmesi yer almaktadır.

Ayrıca Tehdit Bilgisi Platformları ile siber tehdit bilgileri diğer paydaşlar ve topluluklarla paylaşılabilmektedir. Tehdit Bilgisi Platformları, güvenlik ekiplerinin tehdit bilgilerini kendi güvenilir çevreleri arasında paylaşmalarını, güvenlik uzmanlarıyla arayüz oluşturmalarını ve eşgüdümlü karşı önlemlerin uygulanması konusunda rehberlik almalarını mümkün kılmaktadır. Tam özellikli Tehdit Bilgisi Platformları, güvenlik analistlerinin bu taktik ve stratejik faaliyetleri olay yanıtı, güvenlik operasyonları ve risk yönetimi ekipleriyle eşzamanlı olarak koordine etmesini sağlarken, güvenilir topluluklardan veri toplamaktadır [35].

Bunun yanı sıra, organizasyonların TIP çözümlerini geliştirirken ve iletirken spesifik gerekliliklerine ve ihtiyaçlarına odaklanması gerekmektedir. Organizasyonların gerekliliklerini kaydetmeleri ve teknoloji platformları tarafından farklı siber aktivitelerin nasıl sağlanacağı üzerinde çalışması gerekmektedir.

Ayrıca TIP geliştiricilerinin ürünlerin son kullanıcılara daha etkili, tehdit sıralaması yapabilme ve alaka düzeyi belirleme konusunda yardımcı olabilecek analiz yeteneklerinin geliştirilmesine odaklanması gerekmektedir. Bu ürünler için esnek ve kullanılabilir güven modelleme işlevlerini sağlaması gerekmektedir.

Diğer taraftan, siber tehdit bilgisinin paylaşımı için kullanılan platformlara ise Malware Information Sharing Platform (MISP), IBM X-Force Exchange, AbuseHelper, Cyber Threat XChange (CTX), Open Threat Exchange (OTX) ve Collaborative Research into Threats (CRITs) örnek gösterilmektedir.

MISP, hedefli saldırıların, tehdit bilgisinin, finansal dolandırıcılık bilgilerinin ve güvenlik açığı bilgilerine ilişkin tehdit göstergelerinin paylaşılması, depolanması ve ilişkilendirmesi amacıyla kullanılan bir tehdit bilgisi platformu olarak tanımlanmaktadır. MISP, bir diğer tanımda ise kötü amaçlı yazılım örnekleri, olaylar, saldırganlar ve bilgi hakkında teknik ve teknik olmayan bilgilerin depolanmasına izin veren etkili bir tehdit göstergesi ve göstergelerden oluşan bir veritabanı olarak tanımlanmaktadır.

MISP platformunda, siber güvenlik göstergelerinin depolanması, paylaşılması, işbirliği yapılması, kötü amaçlı yazılım analizi işlemleri ile birlikte aynı zamanda kritik altyapılara, kuruluşlarına veya insanlara yönelik saldırıların, dolandırıcılık faaliyetlerinin veya tehditlerin tespit edilmesi ve önlenmesi amacıyla tehdit bilgileri kullanılmaktadır.

MISP platformunda, farklı MISP platformları arasında olayların otomatik olarak senkronize edilmesine ve her kuruluşun paylaşım politikasını karşılamak amacıyla gelişmiş filtreleme işlevlerinin sunulmasına yönelik işlevler sunulmaktadır. Ayrıca olaylar ve olayların korelasyonları arasında inceleme yapılması amacıyla grafiksel bir arayüz imkânı sunulmakta, analistlerin olaylara katkıda bulunmalarına yardımcı olmak amacıyla gelişmiş filtreleme işlevleri ve uyarı listesi sunulmaktadır [36].

IBM X-Force Exchange, tehdit bilgisi kullanılması, paylaşılması ve bunlara yanıt verilmesi amacıyla kullanılan bir bulut platformu olarak tanımlanmaktadır. En son küresel güvenlik tehditlerinin hızlı bir şekilde belirlenmesi, işlem yapılabilir bilginin bir araya getirilmesi ve sektördeki paydaşlarla işbirliği yapılmasına olanak tanımaktadır.

IBM X-Force Research platformu üzerinden tehdit bilgisi içeriği sağlanarak çeşitli kaynaklardan gelen güvenlik sorunları izlenmekte ve analiz edilmektedir. IBM X-Force, müşterilerine, araştırmacılara ve genel olarak topluma en son güvenlik risklerini daha iyi anlamalarına ve ortaya çıkan tehditlerden daha önde olmalarına yardımcı olmaktadır.

Söz konusu platform aracılığıyla; çok sayıda tehdit bilgisine erişim sağlama, tehdit bilgisi paylaşılması, tehditlerin hızlı bir şekilde durdurulması için entegre çözüm sunulması, sonuçların düzenlenmesi ve açıklanması için kullanımı kolay arayüz imkanı, izleme listelerinin kullanılarak geçerli göstergelerin kontrol edilmesi konularında işlev sunulmaktadır [37].

AbuseHelper, olay bildirimlerini otomatik olarak işlemek amacıyla CERT.FI ve CERT.EE tarafından ClarifiedNetworks ile başlatılan açık kaynaklı bir proje olarak tanımlanmaktadır. Söz konusu araç, Bilgisayar Olaylarına Müdahale Ekibi **(**CERT**)** ekipleri için çok çeşitli yüksek hacimli bilgi kaynaklarını takip etme ve iyileştirme için geliştirilmiştir.

2012 yılında kurulan Open Threat Exchange (OTX) platformu, siber saldırıları yönetmek için ticari ve açık kaynak çözümleri geliştiricisi olan AlienVault tarafından geliştirilmiştir. OTX platformu, virüsler, kötü amaçlı yazılımlar ve diğer siber saldırılar hakkında bilgi paylaşan bilgisayar korsanlarına karşı mücadele edilebilmesi amacıyla oluşturulmuştur. 140 ülkede günde 19 milyondan fazla potansiyel tehdidi paylaşan 80.000'den fazla katılımcısı bulunmaktadır. OTX platformu bulut tabanlı bir platform olup, bilgi paylaşımı, virüsler, kötü amaçlı yazılımlar, izinsiz giriş tespiti ve güvenlik duvarları gibi güvenlikle ilgili çok çeşitli sorunları kapsamaktadır. Otomatik araçlar sayesinde, katılımcılar tarafından paylaşılan veriler toplanmakta, doğrulanmakta ve yayınlanmaktadır.

Collaborative Research into Threats (CRIT) ise tehdit savunması yapan analistler ve güvenlik uzmanları için birleşik bir araç oluşturmak üzere diğer açık kaynaklı yazılımlardan yararlanan açık kaynaklı bir kötü amaçlı yazılım ve tehdit deposu olarak tanımlanmaktadır. CRIT, 2010 yılından bu yana geliştirilmekte olup, güvenlik topluluğuna tehdit verilerini analiz etmek ve üzerinde çalışmak için esnek ve açık bir platform sunmayı hedeflemektedir.

Bunun yanı sıra, etkili bir tehdit bilgisi çözümünün birden fazla veri akışından faydalanması gerekmekte, tam özellikli bir tehdit bilgisi çözümünün, verilerini kısıtlı bir kaynak kümesinden üretilmemesi gerekmektedir. Örneğin, ThreatTrack firması çalışanı Corlette'e göre, ürünlerinin 80'den fazla farklı paylaşım ortağından bilgi topladığı, bunlar arasında; açık kaynaklı yayınlar, ortaklardan toplu yayınlar, tehdit aktörleri hakkında bilgiler, kötü amaçlı yazılımların davranış analizi, e-posta listeleri, bültenler, sosyal medya ve tehdit bilgisi kütüphaneleri gibi kaynakların bulunduğu belirtilmektedir.

Tehdit bilgisi sağlayıcısının tüm bu verileri topladıktan sonra, işlem yapılabilir hale getirmek için gereken bağlamı sağlamak amacıyla bilgileri iyileştirmesi ve doğrulaması gerekmektedir. Potansiyel tehdit bilgisinin birçok kaynağı karmaşık olduğundan, gelen tüm ham verilerin iletilmeden önce yeniden doğrulanmasına dikkat edilmesi gerekmektedir.

2.5. Siber Tehdit Bilgisi Paylaşımı

Yeni siber saldırı modellerinin belirlenebilmesi ve gelişmiş siber saldırganların hızına ayak uydurabilmek için yeni savunma yaklaşımlarının geliştirilmesi önem arz etmektedir. Siber tehditlerle etkili bir şekilde müdahale edebilmek amacıyla siber ortamdaki tehditlere ilişkin gerekli bilgilerin zamanında elde edilmesi ve işlenmesi gerekmektedir. Ancak organizasyonlar sahip oldukları siber tehdit bilgisi ile belirli nicelik ve nitelikteki tehditleri tespit edebilmektedir. Bu kapsamda, organizasyonlar siber ortamda diğer paydaşların bilgi birikimine, deneyimlerine ihtiyaç duymakta ve işbirliği çabalarını genişletmektedir. Zira siber tehdit bilgisinin işlevselliği, tehdit bilgilerinin paydaşlar arasında paylaşılması ile maksimize edilebilmektedir [8].

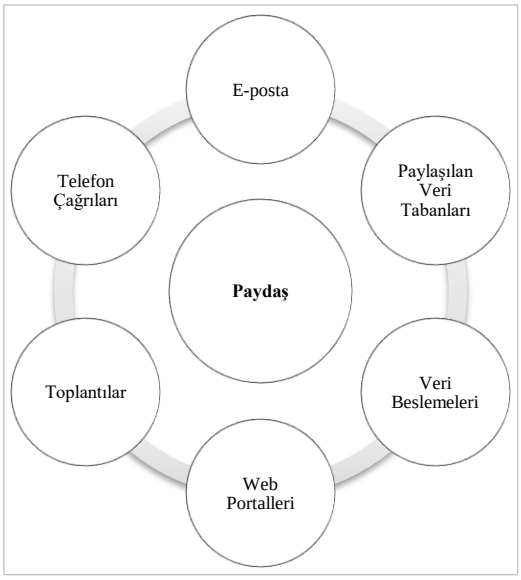
Siber tehdit bilgisi paylaşımı, paydaşlar arasında durumsal farkındalığı artırmak amacıyla yeni bir metot olarak ortaya çıkmıştır. Tehdit bilgisi paylaşımındaki temel amaç, yeni tehditler ve zafiyetlere yönelik paydaşlar arasında durumsal farkındalığı oluşturmak, artırmak ve hızlı bir şekilde yeni tedbirlerin alınmasını sağlamaktır [1]. Çizelge 2.2'de organizasyonlarda kurumsal siber güvenliğin sağlanması için siber tehdit bilgi paylaşımına duyulan ihtiyaçlar ve siber tehdit bilgi paylaşımının organizasyonların kurumsal siber güvenliğine sağlayacağı avantajlar listelenmiştir. Organizasyonlar, sahip oldukları siber tehdit bilgilerini paylaştıkça siber tehditler hakkında en güncel bilgiye sahip olabilecek ve siber tehditlere yönelik gerçek zamanlı önlemler alabilecektir.

Çizelge 2.2. STB paylaşımına duyulan ihtiyaç ve STB'nin avantajları

STB Paylaşımının Faydaları	STB Paylaşımına Duyulan İhtiyaç
▪ Bilgi, deneyim ve tecrübe paylaşımı sağlanabilmekte ▪ Siber tehditlere karşı topyekûn mücadele edilebilmekte ▪ Siber tehditler hakkında en güncel bilgiye sahip olunabilmekte ▪ Tehditleri algılama, öngörme ve saldırılarla birlikte mücadele etme yetenekleri geliştirilebilmekte ▪ Gerçek zamanlı önlemler alınabilmekte ▪ Tehditlere karşı hız ve zaman kazanılabilmekte ▪ Kaynaklar zenginleştirilebilmekte ▪ Durumsal farkındalık artırılabilmekte ▪ Etkileşim ve fikir paylaşımı sağlanabilmekte ▪ Erken uyarı ve müdahale yeteneği kazanılabilmekte ▪ Dijital ekosistemin direnci artırılabilmekte ▪ Paydaşlarla güvenilir bağlantılar kurulabilmekte ▪ Paydaşlar arasında güven duygusu artırılabilmekte ▪ İtibar kayıpları ve marka hasarları engellenebilmekte	▪ Siber tehdit bilgilerinin elde edilmesinin zor olması, uzman bilgisine ihtiyaç duyulması, uzun ve zahmetli çalışma sürecine ihtiyaç duyulması ▪ Tehditler hakkında yeterli bilgiye sahip olunamaması ▪ Tehditler hakkında en güncel bilgilerin elde edilememesi ▪ Siber tehdit bilgilerinin çok hacimli ve/veya karmaşık olması ▪ Fazla iş yükü gerektirdiğinden zaman ayrılamaması ▪ Farklı raporlar üzerinden siber tehdit bilgisi oluşturmanın güç olması ▪ Yamaları önceliklendirmenin zor olması ▪ İncelenmesi gereken çok fazla uyarının bulunması ▪ Zararın ve ek ihlallerin tespit edilmesinin zor olması ▪ Yanlış değerlendirilmiş bilgiler elde edilebilmesi ▪ Doğrulanmamış bulguların hatalı alarmlara neden olması ▪ Elde edilen bilgilerin güvenilir olduğundan emin olunamaması

Çizelge 2.2.'de görüldüğü üzere, siber tehdit bilgisi gelişen tehdit örüntülerinin belirlenmesi ve saldırıların önlenebilmesi bakımından önemli bir araç olarak ortaya çıkmakta olup, organizasyonlar elde edecekleri siber tehdit bilgisi ile siber tehditlere yönelik gerekli önlemleri alabilecektir. Kapsamlı ve standartlaştırılmış bilgi paylaşımı ise organizasyonlara siber tehditlerle daha etkin mücadele edilmesine olanak sağlamakta ve siber saldırılar henüz gerçekleşmeden engellenebilmektedir.

Öte yandan, tehdit bilgisi paylaşımında dikkat edilmesi gerekilen bazı hususlar bulunmaktadır. Efektif bir siber tehdit bilgisi paylaşımı güvenilir olmalı, sürdürülebilir olmalı ve hızlı bir şekilde özelleştirilebilmeli, doğru etiketleme yapılmalı, anonim olmalı, güven sağlamalı ve gizli olmalıdır [1]. Ayrıca paylaşım ağının otomatize olması ve sektör bazlı spesifik paylaşım gruplarının oluşturulması gibi dikkat edilmesi gerekilen bazı hususlar bulunmaktadır. Otomatize veri analizi, işbirliği ve siber tehdit bilgisi paylaşımı, siber saldırılarla mücadelede çok önemli bir role sahiptir. Otomatize siber tehdit bilgisi paylaşımının amacı, paylaşım sürecini basitleştirmek ve hızlandırmak, dokümante etmek, değerlendirmek ve güvenlik bilgilerinin düzeltilmesini sağlamaktır [1]. Otomatikleştirilmemiş paylaşım yöntemleri, güvenlik açıklıkları hakkında bilgi alışverişinde yaygın olarak kullanılan yaklaşımlardır. Şekil 2.2'de görüldüğü üzere otomatize olmayan tehdit bilgisi paylaşımı; e-postalar, telefon çağrıları, web portalleri, paylaşılan veritabanları ve veri beslemeleri üzerinden gerçekleştirilmektedir.



Şekil 2.2. Otomatize olmayan STB paylaşımı [1]

Ancak otomatize olmayan veri işleme süreçleri yoğun emek ve zaman kaybına neden olmakta ve bilgilerin önemini yitirmesine sebep olmaktadır. Yeni tehditlerin işlenmesi esnasında hata oranının artması veya ilgi düzeyine göre filtreleme yapılabilmesi nedenleriyle otomatize olmayan sistemler siber tehdit bilgisi paylaşımının etkinliğini azaltabilmektedir.

Moriarty tarafından yapılan çalışmada, siber tehdit bilgisi paylaşımının iki önemli bileşeni iki adımda tanımlanmıştır. Siber tehdit bilgisi paylaşımı, ilgili ve eyleme geçirilebilir olmalı, tehdit paylaşım modeli ise hızlı, ölçeklenebilir ve otomatize olmalıdır [38]. Siber tehdit bilgisi verilerinin otomatize bir şekilde değerlendirilmesi, organizasyon içinde üretilen alarmlarla ve organizasyon dışından temin edilen bilgilerin etkin bir şekilde kullanılabilmesi amacıyla önem teşkil etmektedir. Otomasyon, siber tehdit bilgisi paylaşımında kilit rol oynamaktadır [39].

Ponemon Instıtute tarafından yapılan araştırmada ise; katılımcıların %39'u otomatize olmayan ve hızlı olmayan paylaşım işlemlerinin katılımcıların tam paylaşımını engellediğini, %24'ü ise hızlı olmayan ve otomatize olmayan paylaşım işlemlerinin tümüyle paylaşımı engellediğini belirtmiştir [40].

Bunun yanı sıra, siber alanda aynı sektördeki farklı organizasyonlar genellikle aynı aktörler tarafından hedef alınmaktadır. Siber suçlara karşı karşılıklı yardım sağlanması ve mümkün olduğunca bu saldırıların tekrarlanmasının önlenmesi için tehdit göstergeleri hakkındaki bilgi paylaşım ağlarının genişletilmesi gerekmektedir. Bu sebeple, organizasyonlar, finans, akademi, otomotiv, elektrik gibi sektör bazlı spesifik paylaşım grupları oluşturulabilmektedir. Bu paylaşım grupları, sektör bazlı spesifik zafiyetleri azaltmaya çaba göstermektedir [1].

Bunun yanında organizasyonlar, diğer paydaşlarla daha çok bağlantı sağlamaya ve diğer paydaşların bilgi ve deneyimlerinden yararlanmaya çaba göstermektedir. Nitekim Shackleford tarafından yapılan bir araştırmada, paydaşların %56'sının siber tehdit bilgisini tedarikçilerden aldığı, %54'ünün genel siber tehdit bilgisi paylaşımlarından yararlandığı, %53'ünün ise açık kaynaklardan tedarik ettiği belirlenmiştir [41].

Ayrıca siber tehdit bilgisi çoğunlukla ulusal düzeyde paylaşılmakta ancak uluslararası bilgi alışverişleri özellikle dünya çapında faaliyet gösteren daha büyük kuruluşlar arasında ivme kazanmaktadır. Nitekim aralarında ABD, AB, Japonya ve Güney Kore'nin de bulunduğu bazı hükümetler bilgi paylaşımını artırmak ve genişletmek amacıyla çeşitli çalışmalar gerçekleştirmektedir [42]. Özellikle devlet destekli siber saldırganlar tarafından hedef alınan organizasyonlar kamuyla yakın bir işbirliği ve paylaşıma ihtiyaç duymaktadır [43]. ENISA'ya göre AB'deki 80 kuruluş ve organizasyon ve 50'den fazla ulusal ve kamu CSIRT ekibi siber tehdit bilgisi paylaşımına dâhil olmaktadır [1]. İngiltere'deki Cyber Information Sharing Platform (CISP) girişimi ise güvenlik olayları hakkında bilgi paylaşımı sağlamak amacıyla pek çok paydaşı barındırmaktadır [6].

Diğer taraftan, organizasyonları tehdit bilgisi paylaşımına teşvik eden bazı unsurlar bulunmaktadır. Bauer ve Eeten'e göre bir organizasyon bir siber saldırının kurbanı olduğunda, itibar kaybı ve bunun sonucunda ortaya çıkan marka hasarı nedeniyle, paydaşları siber güvenliğe ve siber tehdit bilgisi paylaşmaya daha fazla yatırım yapmaya teşvik edebilmektedir [44]. Başarıyla savunulan bir ağ, hizmetin çalışma süresine ve sürekliliğine katkıda bulunabilmektedir.

Murdoch ve Leaver'a göre paylaşıma katılma, paydaş itibarı ve ortak amaç olmak üzere siber güvenlik ekiplerini siber güvenlik bilgilerini paylaşmaya motive eden üç ana faktör bulunmaktadır. Ayrıca paydaşların gelecekteki bir siber tehdidi önlemeye yardımcı olması amacıyla paydaşlarla ilgili bilgileri paylaşmak isteyebileceği, sektörde diğer paydaşlar tarafından saygınlığı kabul edilen bir paydaş olmak isteyebileceği ve aynı sektörde çalışan paydaşların kendilerini ortak bir tehdide karşı savunmalarına yardımcı olmak için bilgi paylaşabileceği belirtilmektedir [6].

Ayrıca paydaşlar arasında saygınlığın artması, paydaşları daha fazla katkıda bulunmaya ve itibarlarını artırmaya teşvik etmektedir. Ancak bir paydaşın saygınlığın artması ile birlikte anonim kalması da olanaksız hale gelmektedir. Anonim bilgi paylaşımları, bir paydaşla ilişkilendirilememesi sebebiyle itibara katkıda bulunamamakta ve paylaşılan bilgi kaynağının saygın olup olmadığına yönelik karar vermeyi zorlaştırmaktadır. Bu nedenle, belirtilen sorunun üstesinden, paylaşılan bilginin diğer alıcı paydaşlar tarafından puanlanması ile gelinebilmektedir. Bu kapsamda, bilgi paylaşımına açık, güvenli ve standartlara dayalı bir yaklaşım sağlanması, organizasyonların paylaşım modellerine

katılım sağlamasına ve kritik ağların güvenliğinin siber tehditlere yönelik korunmasına imkân tanımaktadır [6].

Bununla birlikte, organizasyonlar, işletmeler ve uzmanlar arasında etkin bilgi paylaşımının olması gerektiği kadar verimli olmadığı vurgulanmakta, kamu kurumları, özel işletmeler ve hatta endüstri uzmanları tarafından yönetilen çok iyi girişimlerin olduğu doğru olsa da, ortak bir bilgi paylaşım standardı olmadığından bu bilgileri paylaşmanın çok zor olabildiği vurgulanmaktadır [45]. Ayrıca özel sektör kuruluşları rekabet, sorumluluk ve yatırım getirisi gibi çeşitli nedenlerden dolayı işbirliği çalışmalarına katılım sağlama konusunda bazen ihtiyatlı davranmakta veya bilgi paylaşım çabalarına katılmaya isteksiz olmaktadır. Bu sebeple siber güvenlik bilgi paylaşımına katılımı teşvik etmek zor olabilmektedir.

Öte yandan, siber tehdit paylaşımı konusunda çeşitli zorluklar bulunmaktadır. İhtiyaç duyulan siber tehdit bilgisinin elde edilmesinin zor olması, yanlış değerlendirilmiş bilgiler elde edilebilmesi, bu kapsamda uzman bilgisine ihtiyaç duyulması, uzun ve zahmetli çalışma sürecine ihtiyaç duyulması, fazla iş yükü gerektirdiğinden şirketlerin ve/veya kurumların siber tehdit bilgisini üretmek için zaman ayırmaması veya ayıramaması, saldırı tespit sistemleri tarafından üretilen raporlar arasında genel bir benzerlik olmayışı ve her bir saldırı tespit sisteminin çıktısının farklı veri modeli barındırması, farklı raporlar üzerinden siber tehdit bilgisi oluşturmanın güçlüğü, doğrulanmamış bulguların hatalı alarmlara neden olması, yamaları önceliklendirmenin zor olması, incelenmesi gereken çok fazla uyarının bulunması, zararı ve ek ihlalleri tespit etmenin zor olması ve yöneticilerin teknik problemler hakkında bilgisinin bulunmaması belirlenen zorluklar arasında yer almaktadır.

Bu kapsamda, siber tehdit bilgisi oluşturmada kullanılan manuel adımların otomatize edilmesi ve standartlaştırılması, ayrıca uzman bilgisine gereksinim duyulmaksızın kolaylıkla siber tehdit bilgisi üretebilme yeteneğinin kullanıcılara kazandırılmasına yönelik mekanizmanın oluşturulmasına ihtiyaç duyulmaktadır.

Bunların yanında, paydaşlar arasında dilsel ve kültürel farklılıklar bulunabilmektedir. Paydaşlar farklı çalışma alanlarında faaliyet gösterebilmekte ve farklı dilleri konuşabilmektedir. Bu da bilginin kalitesi üzerinde olumsuz etki oluşturmaktadır [46]. Siber tehdit bilgisi paylaşımı küresel olarak gerçekleştirilmekte ve paydaşlar arasında kültürel ve dilsel engellere sebep olabilmektedir. Paylaşım modelinde ortak bir paylaşım

dili tanımlanmalı ve kültürel yönleri anlaşılmalıdır. Ayrıca aynı dilin konuşulması, paydaşları bilgi paylaşımına teşvik edebilmekte ve bilgi paylaşım sürecini hızlandırabilmektedir [47]. Bunun yanı sıra, çeviride bazı temel özellikler kaybolabilmekte ve siber tehdit bilgilerinin kalitesini ve ilgi düzeyini düşürebilmektedir. Zira paylaşım dilinin paydaş tarafından anlaşılamaması durumunda zaman alıcı bir çevirinin başlatılması gerekebilmektedir.

Bununla birlikte, siber tehdit bilgisi işbirliği bazı güvenlik risklerini barındırmaktadır. Haustein ve arkadaşları, bir olayla ilgili organizasyon içi bilgilerin ifşasının bir paydaşın itibarına zarar verebileceği endişelerini dile getirmektedir [48]. Ayrıca pek çok organizasyon, markalarını olumsuz etkileyebilecek bilgileri paylaşmaktan kaçınmakta, bazı şirketler ise saldırı bilgilerinin ifşa edilmesinden kaynaklanabilecek itibar zedelenmesi korkusu nedeniyle bilgi paylaşmakta tereddüt edebilmektedir. Bunun yanı sıra, bir rakip tarafından elde edilen siber tehdit bilgisinin sistemlerine henüz yama uygulamamış paydaşlara saldırmak için kullanılabileceği vurgulanmaktadır [49]. Buna ilave olarak siber tehdit bilgisini rakiplerle paylaşmak, ücretsiz bilgi edinmeyi teşvik edebilmekte, bu çerçevede paydaşlarla veya topluluklarla bilgi paylaşılmamasına yol açabilmekte, güven ihlal edilebilmekte ve olumsuz tanıtım marka itibarını etkileyebilmektedir. [48]

Öte yandan, çok sayıda siber tehdit bilgisi kaynağının olması sebebiyle çok sayıda veri akışı olabilmekte, siber saldırıya karşı savunma yapılabilmesi amacıyla paydaşların ilgili, eyleme geçirilebilir tehdit bilgisine zamanında erişmesi ve bu doğrultuda hareket etmesi önem teşkil etmektedir. Ponemon Enstitüsü tarafından 2016 yılında yapılan ve 1000 katılımcının katılım sağladığı bir ankete göre, katılımcıların %70'i tehdit bilgisinin eyleme geçirilebilir bilgi sağlamak için çok hacimli veya karmaşık olduğunu belirtmiştir. Katılımcıların %80'inin tehdit bilgisi platformunun kurulmasının organizasyonun tehdit bilgisini otomatikleştirmesine yardımcı olabileceğini düşündüğü, %54'ünün ise tehdit bilgisi potansiyelini tam olarak kullanmak için nitelikli bir tehdit analisti kadrosuna sahip olmasının gerektiğini ifade etmiştir [5].

Siber tehdit bilgisi paylaşımında karşılaşılan diğer bir sorun ise tehdit verisinin kalitesidir. Ponemon Ensititüsü tarafından yapılan çalışmada, katılımcılar tarafından tehdit bilgisi beslemelerinin %70'inin işlenmemiş olduğu ve kalite açısından güvenilir olmadığını belirtilmiştir. Siber tehdit bilgisi sağlayıcısının, tehdit bilgisinin değerinin artırmasına ve

eyleme geçirilebilir hale getirilmesine yardımcı olmak amacıyla verileri zenginleştirmesi gerekmektedir.

Sonuç itibarıyla, standart veri yapıları ve taşıma protokolleri, birlikte çalışabilirliğin önemli elementleridir. Yaygın formatların ve protokollerin kullanılması, bilgi paylaşımının otomatize hale gelmesine imkân sağlayabilmekte ve hız kazandırabilmektedir. Bununla birlikte, belirli formatların ve protokollerin benimsenmesi, önemli zaman ve kaynaklar gerektirebilmekte ve paydaşlar tarafından farklı yapıların veya protokollerin gerekmesi halinde bu yatırımların değeri önemli ölçüde azaltılabilmekte, yeni imkân ve kabiliyetlerin kazandırılmasına gerek duyulabilmektedir.

2.6. Siber Vatan ve Bilgi Paylaşımı

İnsanlık tarihinin ilk zamanlarında savaşlar kara ve denizlerde gerçekleşmiş, 20. yüzyılın başından itibaren hava, 1950'lerden itibaren ise uzay yeni harp alanları olarak ortaya çıkmıştır. Geleneksel olarak konvansiyonel harbin kara, hava, deniz ve uzay olmak üzere 4 boyutu bulunmaktadır. Teknolojinin gelişmesi ve kara, deniz, hava ve uzayda bilişim sistemlerinin kullanımının artması ile birlikte siber uzayın önemi daha da artmış, siber uzay, kara, hava, deniz ve uzaydan sonra harbin beşinci boyutu olarak ortaya çıkmıştır. Siber uzay, internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyicileri içeren ve birbirine bağlı bilgi sistemleri altyapıları ağından oluşan bilgi ortamındaki küresel alan olarak tanımlanmaktadır [50].

Siber uzay günümüzde dijital çağda harbin ayrılmaz bir parçası haline gelmiş ve geleneksel harbin yerini siber savaşlar almaya başlamıştır. Değişen tehdit ortamı, ülkelerin ve uluslararası güvenlik organizasyonlarının da gündemine girmiş, bu yönde strateji geliştirilmeye başlanılmıştır. Nitekim siber uzay ve siber savaş gibi konular NATO'nun da güvenlik stratejileri kapsamına alınmıştır. NATO, 2016 Varşova Zirvesi'nde siber uzayı, kara, deniz, hava ve uzay gibi bir harekât alanı olarak tanımlamıştır [51]. Ayrıca, NATO'nun yeni güvenlik konseptinde mücadele edilmesi gereken öncelikli alanlar içerisinde yer alan "siber güvenlik alanında üye ülkelerin daha fazla işbirliği içerisinde olması gerektiğine ve diğer uluslararası kuruluşlar ve ortak ülkelerle olduğu kadar sanayi ve akademi ile işbirliğinin geliştirileceğine" vurgu yapılmıştır [52].

Siber uzay, internet ve internete bağlı bilgi sistemlerini kapsamakta olup, son dönemde ortaya çıkan Nesnelerin İnterneti gibi teknolojiler ile birlikte siber uzayın sınırları bilgisayarlarla sınırlı kalmayarak daha da genişlemiştir [53]. Siber ortam ve bilişim sistemlerinin kullanım oranı gittikçe artmakta ve büyük bir dijital dönüşüm yaşanmaktadır. Mevcut teknolojilerin yanı sıra yapay zekâ, Nesnelerin İnterneti, blokzincir ve 5G teknolojilerin hayatımıza girmesi ile birlikte dijital dönüşüm sürecinde büyük ilerlemeler kaydedilmiştir. Pek çok ülke ve organizasyon, bu dönüşüme cevap vermeye, gelişen yeni yetenekleri etkinleştirmeye, bu yeteneklerle organizasyonların ihtiyaçlarını desteklemeye ve gelişmelerin gerisinde kalmamaya, teknolojinin imkânlarından en üst düzeyde yararlanmaya gayret göstermektedir.

Dijitalleşmenin ve siber alanın boyutlarının genişlemesi ile birlikte günümüzde egemenliklerin dijital dünyada siber saldırılara maruz kaldığı görülmektedir. Güvenlik kavramı geleneksel yapısından farklı olarak sanal dünyada da etkisini göstermekte ve siber uzayda kullanılan siber silahlar da konvansiyonel silahlar gibi yeni bir unsur olarak kullanılmaya başlanmıştır. Nitekim siber uzayda, bilişim sistemlerindeki verilere erişim sağlanması, kişisel veya kurumsal bilgilerin çalınması, yayılması veya bilgi sistemlerinin çalışamaz hale gelmesi ile neticelenebilecek saldırılar yaşanabilmektedir. Ayrıca hayatın devamlılığının sağlanması için büyük öneme sahip kritik altyapı sektörlerinin hedef alındığı saldırılar ile elektrik şebekelerinin, su dağıtım/arıtma tesislerinin, elektronik haberleşme ve finans altyapısının çalışamaz hale gelmesine neden olabilecek ve toplumuzun tüm kesimlerini etkileyebilecek sonuçlar ile karşılaşabilmektedir. Bu sebeple, devletlerin kritik altyapı sektörleri başta olmak üzere siber alandaki varlıklarını koruması, önemli bir güvenlik unsuru haline gelmiştir.

Günümüzde siber uzayın savunulmasına yönelik pek çok çaba gösterilmekte, bu çabalar ortaya konulan stratejiler, politikalar ve doktrinler ile desteklenmekte, ayrıca öne sürülen yeni kavramlar ile siber uzayın önemi vurgulanmaktadır. Son zamanlarda ortaya çıkan "Siber Vatan" kavramı ise siber tehditlerden korunması açısından büyük önem teşkil etmektedir. "Vatan" veya "Yurt" kelimesi sözlükte bir halkın üzerinde yaşadığı, kültürünü oluşturduğu toprak parçası olarak ifade edilmektedir. Vatan kelimesi ayrıca "yerleşmek, bir yeri yurt edinmek, kendini bir şeye alıştırmak" anlamındaki "vatn" kökünden türemekte, aynı zamanda "kişinin doğduğu, yerleştiği, barındığı ve yaşadığı yer" anlamına gelmektedir. Bununla birlikte, literatürde "Siber Vatan" kavramına ilişkin yapılmış henüz

bir tanım bulunmamaktadır. Siber alanda yaşanan gelişmeler ve gelişen siber tehdit ortamı göz önüne alındığında "Siber Vatan" kavramına ilişkin "bir ülkeye ait bilgi, iletişim altyapısı ve sistemlerinin bulunduğu, kamu kurumlarına, şirketlerine ve vatandaşlarına ait verilerinin üretildiği, depolandığı, işlendiği veya iletildiği siber ortam" şeklinde bir tanım yapılabileceği değerlendirilmektedir. Siber ortamda bulunan ve ülkemize veya vatandaşlarımıza ait olabilecek her bilişim sistemi, veri veya siber varlık Siber Vatanın birer parçası olarak değerlendirilebilmektedir.

Siber Vatanın, ana vatanın bir parçası olduğu göz önünde bulundurularak "Siber Vatan" kavramının doğru anlaşılması gerekmektedir. Siber Vatanı da ana vatan kavramında olduğu gibi algılamamız, Siber Vatanı korumamız, ülkemize ait bilişim sistemlerini ve altyapılarını, bilgi varlıklarını, ülkemizdeki tüm kuruluşlar ve vatandaşlarımıza ait verilerin güvenliğini sağlamamız gerekmektedir. Bu çerçevede, öncelikle Siber Vatanın sınırları belirlenmeli ve bu sınırlarının korunması için çalışmalar gerçekleştirilmelidir. Bu dijital sınırlar içerisinde yer alan tüm varlıkların bilinmesi ve bu varlıkların Siber Vatan kavramı kapsamında savunulması, siber uzayı kullanan tüm kullanıcılarda ise bu farkındalığın oluşturulması, tüm kullanıcıların siber ortamdaki varlıklarını korumaya yönelik en üst düzeyde hassasiyet göstermesi, verilerine ve varlıklarına sahip çıkması ve dijital sınırlarımızın topyekûn korunması gerekmektedir.

Ayrıca siber uzayda, geleneksel komşularımızdan farklı olarak tüm dünya ile komşu olduğumuzun farkında olunması, gelişen tehdit ortamı ve riskler belirlenerek Siber Vatan kavramı çerçevesinde siber savunma stratejilerinin geliştirilmesi, siber varlıklarımızı koruyacak stratejilere, teknolojilere, altyapılara, merkezlere, araçlara, platformlara, insan kaynağına ve eğitimlere odaklanılması, kamu-özel-akademi arasında işbirliği çalışmalarının gerçekleştirilmesi gerekmektedir.

Öte yandan, içinde bulunduğumuz bilişim çağında ekonomik, sosyal, kültürel ve teknolojik alanlardaki hızlı değişimler geleneksel güvenlik anlayışında da bazı değişimlere neden olmuş, siber ortamdaki tehditlere yönelik gerekli güvenlik önlemlerinin alınması ve Siber Vatandaki varlıkların korunması ihtiyacı ortaya çıkmıştır. Bu kapsamda, Siber Vatanda güvenliğin sağlanması amacıyla yapılması gereken çalışmaların belirlenmesi ve bu doğrultuda gerekli önlemlerin alınması gerekmektedir. Bu çerçevede, Siber Vatanda tehdit bilgisi paylaşımı konusunda gerçekleştirilmesi gerekilen çalışmaların belirlenebilmesi ve

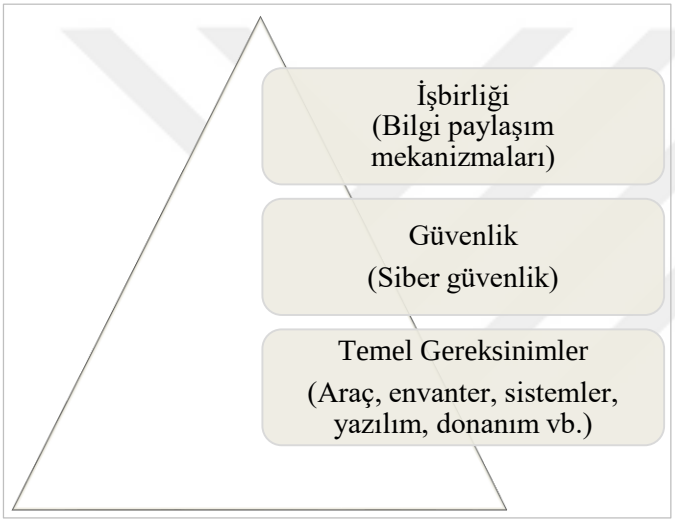
bu konudaki eksikliklerin tespit edilebilmesi amacıyla Maslow'un İhtiyaçlar Hiyerarşisi ve Zack Bilgi Boşluğu analizinde faydalanılmıştır.

Amerikalı psikolog Abraham Maslow tarafından 1943 yılında geliştirilen Maslow'un İhtiyaçlar Hiyerarşisinde, insanların temel gereksinimlerini karşıladıktan sonra güvenliğini sağlamaya yönelik çaba gösterdiği, güvenlik konusunun temel gereksinimlerden sonra insanlar için bir ihtiyaç olarak ortaya çıktığı öne sürülmektedir. İnsanların belirli kategorilerdeki ihtiyaçlarını karşıladıktan sonra daha üst ihtiyaçları karşılama arayışına girdiğini belirten Maslow'un İhtiyaçlar Hiyerarşisi, fizyolojik gereksinimler, güvenlik gereksinimi, sevgi, gereksinimi, saygınlık gereksinimi ve kendini gerçekleştirme gereksinimi aşamalarından oluşmaktadır [54]. Şekil 2.3.'te Maslow'un İhtiyaçlar Hiyerarşisinde yer alan aşamalar belirtilmiştir.

Şekil 2.3. Maslow'un İhtiyaçlar Hiyerarşisi [54]

Bu hiyerarşide insanlar, temel gereksinimlerini sağladıktan sonra güvenlik gereksinimlerini karşılamaya çabalamaktadır. Bireylerin güvenli bir ortamda yaşama istekleri bir ihtiyaç olarak karşımıza çıkmakta, bireyler hayatta kalabilmek amacıyla temel gereksinimlerini karşıladıktan sonra güvenli bir hayat sürdürebilmeyi hedeflemektedir. Maslow Hiyerarşisinde ilk iki basamak sosyal bir varlık olan insan için olmazsa olmazlar arasında yerini almaktadır. Hiyerarşide üst basamaklara çıkıldıkça fiziksel ihtiyaçlar yerini sosyal ihtiyaç ve isteklere bırakmaktadır.

Maslow'un İhtiyaçlar Hiyerarşisi, Siber Vatan kavramı kapsamında değerlendirildiğinde, Siber Vatanda yürütülen faaliyetlerin güvenli ve kesintisiz bir şekilde sürdürebilmesi amacıyla Siber Vatan için gerekli olan temel gereksinimler karşılandıktan sonra bu alanda güvenliğin sağlaması ve siber tehditlere yönelik Siber Vatanın içinde yer alan varlıkların korunması gerektiği değerlendirilmektedir. Ayrıca Siber Vatanın topyekûn savunulabilmesi ve tehditlerle daha etkin mücadele edilebilmesi amacıyla güvenlik çalışmaları ile birlikte Siber Vatandaki diğer paydaşlarla işbirliği çalışmalarının geliştirilmesi gerektiği düşünülmektedir. Şekil 2.4.'te Maslow'un İhtiyaçlar Hiyerarşi analizi kapsamında Siber Vatanda gerçekleştirilmesi gerekilen çalışmalar belirtilmiştir.



Şekil 2.4. Siber Vatana dair Maslow'un İhtiyaçlar Hiyerarşisi analizi

Bu çerçevede, Siber Vatanda yer alan bilişim sistemlerindeki güvenlik açıklıklarına odaklanılabilmesi ve siber saldırganların saldırıları hakkında bilgi elde edilebilmesi için siber tehdit bilgisine sahip olunması, bu bilgilerin diğer paydaşlarla paylaşılması ve bu bilgiler doğrultusunda savunma çabalarının gerçekleştirilmesi gerekmektedir. Ayrıca benzer sektörleri hedef alan tehdit aktörleri genellikle benzer saldırı metotlarını kullanmaktadır. Bu çerçevede, aynı sektörde faaliyet gösteren paydaşların kendilerini ortak bir tehdide karşı savunmaları, birden fazla kaynaktan gelen siber tehdit bilgisinin analiz edilerek mevcut bilginin artırılması ve tehditlerin yayılmasının önlenmesi amacıyla Siber Vatanda tehdit göstergeleri hakkında bilgi paylaşımının gerçekleştirilmesi ve bilgi paylaşım ağlarının genişletilmesi gerekmektedir. Siber Vatanda bilgi paylaşımını artıracak işbirliği mekanizmalarının ve siber güvenlik ekosisteminin oluşturulması, Siber Vatanın savunulması bakımından önem teşkil etmektedir.

Sonuç itibarıyla, Siber Vatan kapsamında olmazsa olmazlardan olan araç, yazılım, donanım, envanter vb. gibi temel gereksinimler karşılandıktan sonra güvenliğe odaklanılması, Siber Vatandaki varlıkların ve sınırların belirlenmesi ve Siber Vatanın topyekun korunması gerekmektedir. Bu kapsamda, politika ve stratejilerin geliştirilmesi, gerekli teknoloji ve altyapılara yatırım yapılması ve bu alanda insan kaynağının artırılması gerekmektedir. Ayrıca Siber Vatanı korurken, siber güvenliğin en önemli unsurlarından biri olan işbirliği çalışmalarına odaklanılması ve işbirliğini teşvik edecek siber güvenlik ekosisteminin oluşturulması ve kamu-özel-akademi arasında işbirliği çalışmalarının artırılması gerekmektedir.

Nitekim Ülkemizin 2020-2023 döneminde başta kritik altyapılarımız olmak üzere siber uzaydaki varlıklarımızın siber tehditlerden korunmasına yönelik gerçekleştirilmesi hedeflenen çalışmalar, Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan 2020–2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında belirlenmiştir. Ülkemizin 2020-2023 dönemi siber güvenlik stratejisi; "siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu ve siber güvenlik alanında belirlenen hedeflere ulaşılabilmesi gerektiği ve kritik altyapılar aracılığıyla verilen hizmetlerin kesintisiz ve etkin olarak sunulmasının esas olduğu" maddeleri temel alınarak belirlenmiştir [55].

2020-2023 dönemi strateji ve eylem planında, "kritik altyapıların siber güvenliğinin sağlanması, yerli ve milli teknolojik kabiliyetlerin geliştirilmesi, proaktif siber savunma anlayışının geliştirilmesi, yeni nesil teknolojilerin güvenliğinin sağlanması, toplumumuzun tüm kesimleri tarafından siber uzayın güvenle kullanılması, siber güvenlik farkındalığının artırılması, paydaşlarla bilgi paylaşımı ve işbirliğinin geliştirilmesi, siber suçların en aza indirgenmesi, internet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesi" kapsamında stratejiler belirlenmiştir [55].

Ülkemizin 2020-2023 dönemi için hazırlanan strateji planında da yer alan ve siber güvenliğin sağlanması için yapılması gereken önemli çalışmalardan biri olan işbirliği ve paydaşlarla bilgi paylaşımı konusu, siber güvenliğin sağlanması için temel ilkelerden birisidir. Siber tehditlerin dinamik yapısına uyum sağlayabilmek ve tehditlerin gerisinde kalmamak amacıyla yeni savunma yaklaşımlarının geliştirilmesi gerekmektedir. Siber güvenlik ekosisteminde tüm paydaşlar kendi siber güvenliğini sağlamak adına çeşitli

çalışmalar gerçekleştirmektedir. Ancak paydaşlar sahip oldukları bilgiler ile belirli kapasitedeki tehditlere yönelik önlem alabilmektedir.

Öte yandan, tehdit bilgisi paylaşımı konusunda Siber Vatanda gerçekleştirilen çalışmalardaki eksikliklerin belirlenebilmesi, "Siber Vatanda ne yapıldığı", "Siber Vatanda ne yapılması gerektiği" ve "Siber Vatanda neler yapılabileceği" hususlarının analizinin gerçekleştirilebilmesi amacıyla Zack Bilgi Boşluğu yaklaşımından faydalanılmıştır.

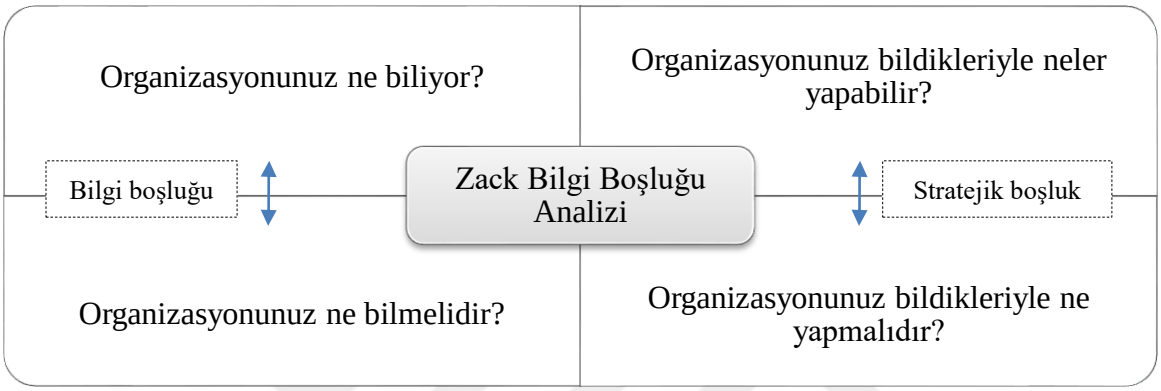
M. Zack'e göre [56, 57];

- Bilgi stratejisine sahip olan bir organizasyon, bilgi stratejisine sahip olmayan diğer organizasyonlara kıyasla farklı değerler üretebilmekte olup, organizasyonlar bilgi kaynaklarını ve yeteneklerini stratejik olarak değerlendirmek için bilgi stratejilerini geniş bir şekilde kavramsallaştırmalıdır.
- Bir organizasyonda hedeflenilen stratejik bilginin elde edilmesi amacıyla stratejik bilgi çerçevesi hazırlanmalı veya analizi yapılmalıdır.
- Bilgiye dayalı kaynaklarının ve yeteneklerinin stratejik bir değerlendirmesini gerçekleştiren bir organizasyon, hangi bilginin geliştirilmesi veya edinilmesi gerektiğini belirlemeli ve mevcut bilgi kategorilerinin stratejik gereksinimleriyle ne ölçüde uyumlu olduğunu değerlendirmelidir.
- Ayrıca organizasyonlar bünyelerindeki sorunları belirleyemediğinde ve stratejilerine yönelik hangi soruları soracağını bilmediğinde bilginin nasıl yönetileceğini bilememektedir. Organizasyonlar, bilmedikleri hususlarla ilgili bilgi sorunlarını tanımalarına ve bunlara yanıt vermelerine yardımcı olacak bilgi yönetimi kılavuzlarına ihtiyaç duymaktadır.

1999 yılında geliştirilen Zack Bilgi Boşluğu analizinde [56];

- Bir organizasyonun "yapabilecekleri" ve "yapılması gerekilenler" arasında nasıl bir denge kurduğu detaylandırılmaktadır. Zack, organizasyonun "bildiği" ve "bilmesi gerekenler" arasındaki farkı bilgi boşluğu olarak tanımlarken, "yapması gerekenler" ve "yapabilecekleri" arasındaki farkı ise stratejik boşluk olarak tanımlamaktadır. (Şekil 2.5)

- Bir organizasyonun yapması gerekenler ile yapabilecekleri arasında bir boşluk olduğu düşünüldüğünde, organizasyonun bilgi güvenliği stratejisini yürütmek için de bilmesi gerekenler ile bildikleri arasında bir boşluk bulunabilmektedir.
- Organizasyonlar bilgiye dayalı kaynaklarının ve yeteneklerinin stratejik bir değerlendirmesini yaptıktan sonra hangi bilginin geliştirilmesi veya edinilmesi gerektiğini belirleyebilmektedir.



Şekil 2.5. Zack Bilgi Boşluğu analizi [56]

Zack Bilgi Boşluğu yaklaşımı kapsamında gerçekleştirilen analiz neticesinde belirlenen ve Siber Vatanda yapılan çalışmalar ve yapılması gerekilen çalışmalar Çizelge 2.3.'te listelenmiştir.

Çizelge 2.3. Siber Vatana dair Zack Bilgi Boşluğu analizi

Siber Vatanda Yapılan Çalışmalar	Yapılması Gerekilenler
▪ 2013-2014, 2016-2019 ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ▪ USOM ve SOME'lerin kurulması ▪ USOM'un siber tehditlere ilişkin bildirim, duyuru ve ikaz faaliyetleri ▪ Siber Güvenlik Kümelenmesinin oluşturulması ▪ Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinin yayımlanması	▪ Siber güvenlik ekosisteminin geliştirilmesi ▪ Siber tehdit bilgilerinin paylaşıldığı işbirliği mekanizmalarının oluşturulması ▪ İşbirliğine yönelik farkındalığın artırılması ve işbirliği kültürünün geliştirilmesi ▪ Paydaşların işbirliğine teşvik edilmesi ve desteklenmesi

Siber Vatan için Zack Bilgi Boşluğu analizi gerçekleştirildiğinde, Siber Vatanda ne yapılabileceği, ne yapılması gerektiği ve ne yapıldığı arasında stratejik boşluk bulunduğu değerlendirilmiş olup, Siber Vatanda tehdit bilgilerinin paylaşılmasına yönelik paydaşlar arasında işbirliğini artıracak çalışmaların gerçekleştirilmesi ile bu stratejik boşluğun giderilebileceği değerlendirilmiştir.

Ülkemizde siber güvenlik çalışmaları Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yürütülmekte olup, Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanmaktadır. Bu eylem planlarında siber güvenlik ekosisteminin geliştirilmesine yönelik kamu-özel sektör-akademi arasında işbirliğinin artırılmasına yönelik eylem maddeleri bulunmaktadır. Ayrıca siber güvenlik ekosisteminin geliştirilmesi amacıyla 2017 yılında Siber Güvenlik Kümelenmesi oluşturulmuş olup, kümelenmede ülkemizde siber güvenlik firmaları arasında işbirliğinin güçlendirilmesi hedeflenmiştir. Bunun yanında, BTK bünyesindeki USOM aracılığıyla siber tehditlere ilişkin bilgi paylaşımı yapılmaktadır.

Gerçekleştirilen analiz neticesinde, siber tehdit bilgilerinin paylaşımı konusunda ülkemizde siber güvenlik ekosisteminin geliştirilmesi gerektiği değerlendirilmiştir. Ülkemizde siber tehdit bilgilerinin paylaşımına yönelik USOM aracılığıyla bilgi paylaşım faaliyetleri gerçekleştirilmekle birlikte, ülkemizde özellikle siber güvenlik firmaları arasında siber tehdit bilgilerinin paylaşıldığı bir işbirliği mekanizması bulunmamaktadır. Ayrıca bu konuda farkındalık ve kültür eksikliği bulunmaktadır.

Sonuç itibarıyla, gerçekleştirilen analizler neticesinde ülkemizde siber tehdit bilgilerinin paylaşıldığı işbirliği platformunun oluşturulması önerilmekte olup, önerilen işbirliği platformu ile Siber Vatanda tehdit bilgilerinin paylaşıldığı işbirliği mekanizması noktasındaki stratejik boşluğun giderilebileceği değerlendirilmektedir.

3. ÖRNEK MODELLER VE ÜLKEMİZDEKİ ÇALIŞMALAR

Siber saldırı tekniklerinin gelişmesi ve bu saldırıların arkasındaki motivasyonların artması ile birlikte bu tehditlerle mücadele edilmesi gittikçe zorlaşmaktadır. Organizasyonlar ise tehditlere ilişkin bilgi ve tecrübelerini artırmayı hedeflemekte ve siber tehditlere yönelik etkin siber savunma metodolojilerinin geliştirilebilmesi amacıyla diğer paydaşların bilgi birikiminden faydalanmayı hedeflemektedir.

Bu çerçevede ABD, AB ve İngiltere'de siber tehdit bilgilerinin paylaşılmasına yönelik işbirliği mekanizmaları bulunmakta olup, tezin bu bölümünde ABD, AB ve İngiltere'de bulunan ve en yaygın modeller olan 3 model incelenmiştir. ABD'de siber güvenlik firmaları arasında bilgi paylaşımı gerçekleştirilmesi amacıyla oluşturulan Siber Tehdit İttifakı (Cyber Threat Alliance), AB'de Kamu Özel İşbirliği Modeli, İngiltere'de ise Siber Güvenlik Bilgi Paylaşım Ortaklığı (Cyber Security Information Sharing Partnership-CISP) faaliyet göstermektedir. Bu bölümün son kısmında ise ülkemizde siber tehdit bilgilerinin paylaşımına yönelik gerçekleştirilen çalışmalar ve siber güvenlik ekosistemi incelenmiştir.

3.1. Amerika Birleşik Devletleri'ndeki Çalışmalar

Amerika Birleşik Devletleri'nde çeşitli siber tehdit bilgisi paylaşım düzenlemeleri bulunmakta olup, bu paylaşım topluluğu düzenlemelerinden bir tanesi Bilgi Paylaşımı ve Analiz Merkezi (ISAC)'dir. ISAC, kritik altyapılara yönelik siber tehditler hakkında bilgi toplanması ve özel sektör ve kamu arasında bilgi paylaşımı sağlanması amacıyla kar amacı gütmeyen bir kuruluş olarak faaliyet göstermektedir. Merkez, siber tehditler, güvenlik açıkları ve siber olaylarla ilgili bilgileri analiz etmekte ve zaman kaybetmeksizin paylaşmaktadır. Bu merkezler aracılığıyla en iyi güvenlik uygulamaları paylaşılmakta ve güvenlik planlaması ve felaket müdahalesi yoluyla dayanıklılık güçlendirilmektedir. Pek çok Bilgi Paylaşımı ve Analiz Merkezinin 7/24 esası ile tehdit uyarısı ve olay raporlama yetenekleri bulunmaktadır [2].

Bilgi Paylaşımı ve Analiz Merkezi kapsamında belirli sektörlerdeki siber güvenliği artırmak ve paydaşlar arasındaki esnekliği geliştirmek amacıyla sektör bazında spesifik bilgi paylaşımı toplulukları oluşturulmuştur. Havacılık, iletişim, acil hizmetler, denizcilik,

finans, sağlık, nükleer, petrol ve doğalgaz, ulaşım ve su gibi çeşitli sektörlerde bilgi paylaşımı toplulukları bulunmaktadır.

Bir başka paylaşım topluluğu düzenlemesi ise Bilgi Paylaşımı ve Analiz Organizasyonu (ISAO)'dur. 2015 yılında ABD'de yayımlanan 13691 sayılı Başkanlık Emri ile siber güvenlik tehdit bilgilerinin özel sektör içinde ve özel sektör ile hükümet arasında paylaşımının geliştirilmesi amacıyla Bilgi Paylaşımı ve Analiz Organizasyonlarının oluşturulması teşvik edilmiştir [58].

ISAO, siber tehdit bilgilerinin toplanması, analiz edilmesi ve paylaşılması amacıyla oluşturulmuş bir gruptur. ISAO, ISAC'den farklı olarak yalnızca kritik altyapı sektörleri ile bağlantılı olmayıp sektörler arası küçük işletmeler gibi topluluklar arasında organize edilmiş bilgi paylaşım faaliyetlerine esnek bir yaklaşım sunmaktadır. Bilgi Paylaşımı ve Analiz Organizasyonları; şeffaflık, kapsayıcılık, uygulanabilirlik ve esneklik olmak üzere 4 temel standardı benimsemektedir [59].

ABD'de yer alan bir diğer bilgi paylaşımı düzenlemesi ise DHS bünyesinde yürütülen Siber Bilgi Paylaşımı ve İşbirliği Programı (CISCP)'dır. Söz konusu program kapsamında kritik altyapı sektörlerinde güvenilir kamu-özel ortaklıkları aracılığıyla eyleme geçirilebilir, ilgili ve zamanında bilgi paylaşımı gerçekleştirilmektedir. CISCP ile paydaşların siber güvenlik risklerini yönetmelerine yardımcı olunmakta ve siber güvenlik olaylarının proaktif olarak algılanması, önlenmesi ve yanıt verilmesi amaçlanmakta, siber güvenlik direncinin oluşturulması hedeflenmektedir. CISP programı kapsamında paydaşlar arasında; gösterge bültenleri, analiz raporları, ortak analiz raporları, kötü amaçlı yazılım ilk bulgu raporları, kötü amaçlı yazılım analiz raporları ve ortak gösterge bültenleri paylaşılmaktadır [59].

Ayrıca DHS, ABD'nin kritik altyapılarının siber tehditlere karşı korunması amacıyla faaliyet göstermektedir. DHS'nin içinde, siber güvenliğe dâhil olan çeşitli ortaklar grubunun çalışmalarını koordine ettiği ve senkronize ettiği merkezi bir konum olarak hizmet veren Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC) bulunmaktadır. 13 federal departman ve ajans ile birlikte 16 özel sektör kuruluşu, merkezde düzenli olarak bağlantı sağlamakta, 100'den fazla özel sektör kuruluşu ise merkez ile rutin olarak işbirliği yapmaktadır. NCCIC, siber güvenlik bilgilerini analiz

etmekte, zamanında ve eyleme geçirilebilir tehdit bilgilerini paylaşmakta ve müdahale, azaltma ve kurtarma çabalarını koordine etmektedir [2].

DHS tarafından yürütülen bir başka gönüllü bilgi paylaşım programı ise Gelişmiş Siber Güvenlik Hizmetleri (ECS) programıdır. Bu program, ticari hizmetleri ve yetenekleri kamu tehdit bilgileriyle tamamlayarak, ABD merkezli kamu ve özel kuruluşlara yönelik gelişmiş bir yaklaşımla koruma ve savunma sağlamaktadır [2].

Diğer taraftan, ABD'de kamu-özel sektör işbirliği ile gerçekleştirilen bilgi paylaşım düzenlemelerinin yanı sıra siber tehdit bilgilerinin özel siber güvenlik firmaları arasında paylaşıldığı Siber Tehdit İttifakı platformu faaliyet göstermekte olup, bu platform kapsamında ABD'deki siber güvenlik şirketleri arasında güncel siber tehdit bilgileri paylaşılmaktadır.

3.1.1. Siber Tehdit İttifakı

Siber ortamdaki kayıplarının engellenebilmesi ve/veya en aza indirgenebilmesi için ABD'de siber güvenlik firmaları arasında güncel tehdit bilgilerinin paylaşılması amacıyla Siber Tehdit İttifakı oluşturulmuştur. 2014 yılında oluşturulan ve 2017 yılında ise bağımsız bir organizasyon olarak yeniden yapılandırılan Siber Tehdit İttifakı, Fortinet, McAfee, Palo Alto Networks ve Symantec firmaları arasında siber tehdit bilgilerinin gerçek zamanlı olarak paylaşılması amacıyla kurulmuştur.

Gelişmiş tehdit paylaşımı için teknoloji, kaynak ve personel platformu olarak tanımlanan Siber Tehdit İttifakı mekanizmasında; bilgi paylaşımını teşvik etmek için paylaşım algoritmasının ve platformunun yönetilmesi, yeni üye alımının desteklenmesi, Siber Tehdit İttifakının misyon ve hedeflerinin desteklenmesi için tanıtım faaliyetleri, bütçe denetim ve Siber Tehdit İttifakı platformunun ve altyapısının geliştirilmesi ve güvence altına alınması kapsamında çalışma alanları bulunmaktadır.

Ayrıca Siber Tehdit İttifakındaki paydaşlar, Siber Tehdit İttifakı komitelerine ve çalışma gruplarına düzenli katılım yoluyla doğrudan birbirleriyle etkileşime girebilmekte, fikirlerini paylaşabilmekte ve kendi çalışmaları ve meslektaşlarının çalışmaları hakkında daha derin içgörüler elde edebilmektedir. Bu düzenli işbirliği aracılığıyla ağda inşa edilen

güven, Siber Tehdit İttifakının üyelerinin bir tehdit, düşman veya faaliyet modeli hakkında daha fazla bilgiye ihtiyaç duyduğu zamanlar için sektör çapında uzmanlar grubu olarak işlev görmesine olanak tanımaktadır [60].

Siber Tehdit İttifakı üyeleri, önceden belirlenmiş alanlara ilişkin ilgili bilgileri STIX paketleri formatında Siber Tehdit İttifakı platformuna yüklemektedir. Tüm STIX 2.0 paketleri en az bir gözlemlenebilir bileşeni içermektedir. Siber Tehdit İttifakı platformunun STIX 2.0 gönderim formatını kullanması, gösterge ve bağlam verilerinin daha kolay paylaşılmasını ve daha iyi okunabilirliğini mümkün kılmakta, bu sayede siber aktörleri caydırma ve paydaşların daha iyi korunmasını sağlamaktadır.

Siber Tehdit İttifakı platformu, üyelerin ihtiyaçlarını karşılayan yüksek kaliteli, eyleme geçirilebilir tehdit bilgisinin paylaşımını teşvik etmek için tasarlanmıştır. Platform, tüm paylaşılan bilgilere değer tabanlı bir algoritma uygulamakta, algoritma zamanlılığı ve ilgili bağlamı değerlendirmekte ve puanlamaktadır. Puanlar, Siber Tehdit İttifakının üyeleri arasında bu verilerin verimliliğine göre verilmektedir.

Platformda iletim esnasında her pakette toplam bir puan değeri belirlenmekte, her paket diğer üyelerin doğrulama amaçlı gönderdikleri bildirimlerle ilişkilendirilmekte ve bir üyenin ortalama günlük puanı belirlenmektedir. Bu paketler; dosya, URI, alan adları ve IP adreslerini içermektedir [61]. Paylaşılan bilgiler, kalitesine göre otomatik olarak puanlanmakta ve üyeler, tehdit bilgisini yalnızca yeterli kalitede girdi sağladıkları takdirde yayımlayabilmektedir. Her pakete gönderim sırasında bir toplam puan değeri atanmakta ve karşılıklı doğrulama için diğer üyelerin gönderimleri ile ilişkilendirilmektedir. Tüm paketler bilgiyi paylaşan üyeye atfedilmekte, ancak etkilenen tüzel kişinin verileri anonimleştirilmektedir. Ayrıca üyeler, yeni veya ilave bilgi eklerken diğer üyeler tarafından daha önce sunulan bilgileri doğrulayarak daha fazla puan almaktadır. Siber Tehdit İttifakının puanlama sistemi, Siber Tehdit İttifakı üyelerinin değer verdiği bilgilerin sunulmasına öncelik vermektedir.

Bir üyenin ortalama toplam günlük puanı, belirlenen minimum değerden büyükse, bu durum o üyenin saygın/itibara sahip olduğunu göstermektedir. Saygın olan üyeler, diğer üyelerin gönderilerini temin edebilmek amacıyla bilgi paylaşan üye, tehdit aktörünün adı ve gönderim tarihi olmak üzere çeşitli filtreler oluşturabilmektedir. Ortalama olarak, üyeler

ayda yaklaşık 5 milyon gözlemlenebilir tehdit (%60 dosya, %40 ağda gözlemlenebilir formatında) paylaşmaktadır. STIX 2.0 paketlerinde ayda yaklaşık 5.000.000 gözlemlenebilir tehdit paylaşılmaktadır.

Bunun yanında, Siber Tehdit İttifakı platformunda paylaşılan STIX paketlerinin en az bir adet Siber Ölüm Zinciri (Cyber Kill Chain) fazı içermesi gerekmektedir. Siber Ölüm Zinciri ise siber saldırının aşamalarını belirlemek ve önlemek için kullanılan metodolojidir. Siber saldırganlar siber saldırıları gerçekleştirmeden önce motivasyonlarına yönelik hedefleri ile ilgili bilgi toplamaktadır. Bu kapsamda, siber saldırıların analiz edilebilmesine yönelik çeşitli modeller bulunmaktadır. Bu modellerden biri olan ve Locheed Martin firması tarafından geliştirilen Siber Ölüm Zincirinde, bir siber saldırının 7 aşamada gerçekleştirildiği belirtilmektedir. Bu aşamalar, keşif (reconnaissance), silahlanma (weaponization), iletim (delivery), sömürme (exploitation), yükleme (installation), komuta & kontrol (command & control) ve eylem (actions on objectives) aşamalarından oluşmaktadır.

Keşif aşamasında, siber saldırganlar hedef sistem ile ilgili bilgi toplamakta olup, saldırganlar tarafından hedef sisteme sızılması için yöntemler araştırılmaktadır. Silahlanma aşamasında, saldırgan tarafından bulunan zafiyetlerin sömürülmesi için yöntem belirlenmekte ve hedef sistemde hangi saldırı vektörünün kullanılacağına karar verilmektedir. İletim aşamasında ise saldırgan tarafından kullanılacak zararlı yazılım hedef sisteme iletilmektedir. Sömürme aşamasında, saldırgan tarafından belirlenen güvenlik zafiyeti sömürülmekte ve saldırganın kullanacağı zararlı yazılımın hedef sistemde çalışması amaçlamaktadır. Yükleme aşamasında, saldırgan tarafından kullanılan zararlı yazılımın sisteme yüklenmesi hedeflenmektedir.

Komuta & kontrol aşamasında ise hedef sistem uzaktan kontrol edilmektedir. Hedef sistem ile komuta & kontrol sunucusu aracılığıyla bağlantı kurulmakta olup, saldırgan tarafından hedef sisteme erişilmektedir. Siber Ölüm Zinciri'nin son aşaması olan eylem aşamasında, sisteme erişim sağlayan siber saldırgan tarafından belirlenen hedeflere ulaşmak için veri çıkarma, silme veya başka bir sisteme saldırma gibi çeşitli eylemler gerçekleştirilmektedir. Ayrıca, asıl hedefine ulaşabilmek için gerçekleştirdiği tüm eylemler bu basamakta değerlendirilmektedir [62].

Küresel dijital ekosistemin siber güvenlik kapasitesinin geliştirilmesi amacıyla faaliyet gösteren Siber Tehdit İttifakının mevcut durumda 31 üyesi bulunmakta ve katkıda bulunan, bağlı üyeler ve kurucu üyeler olmak üzere üç tür üye içermektedir [61]. Siber Tehdit İttifakı üyeleri Çizelge 3.1.'de listelenmiştir.

Çizelge 3.1. Siber Tehdit İttifakı üye listesi [61]

Kurucu Üyeler	Check Point Software Technologies	McAfee
	Cisco	Palo Alto Networks
	Fortinet	
Bağlı Üyeler	NTT Security	Dragos
	Rapid7	IntSights
	Symantec	Juniper Networks
	SK Infosec	NEC Corporation
	Sophos	Anamoli
	Avast	Eleven Paths
	Scitum	Security Scorecard
	Tehtris	Verizon
Katkıda Bulunan Üyeler	AlienVault	Radware
	SonicWall	ReversingLabs
	K7 Computing	Netscout
	OneFirewall	Panda
	SecureBrain	Wmware

Siber Tehdit İttifakında paydaşların plaftorma anlamlı bir katkı yapması beklenmektedir. Bağlı üyeler ittifakın operasyonlarına katılmakta, Yönetim Kurulunda yer almaya hak kazanmakta ve tehdit bilgisi paylaşmakta ve almaktadır. Katkıda bulunan üyeler ise Siber Tehdit İttifakı platformuna daha az mali katkı sağlamakta, üyelik ücreti, üyenin küresel yıllık gelirine bağlı olarak değişmektedir. Katkıda bulunan üyeler, tehdit bilgisi paylaşmakta ve almakta ancak Yönetim Kurulunda yer almaya veya Siber Tehdit İttifakının daimi komitelerinde belirlenmiş bir katılımcıya sahip olmaya hak kazanamamaktadır. Üyelerin sahip oldukları roller Çizelge 3.2.'de belirtilmiştir.

Çizelge 3.2. Üyelerin sahip oldukları roller [61]

Roller	Katkıda Bulunan Üye	Bağlı Üyeler	Kurucu Üyeler
Bilgi paylaşımı ve CTA platformundan bilgi alma, bilgi paylaşım faaliyetlerine katılma	+	+	+
Kötü niyetli siber faaliyetlerin engellenmesi	+	+	+
CTA Yönetim Kurulunda temsil edilebilme	-	+	+
CTA Yönetim Kurulu'nda garantili, süresi sınırlı olmayan bir üyelik elde edilmesi	-	-	+

Siber Tehdit İttifakı ve üyeleri, kötü niyetli aktörlerin araçlarının ve altyapısının genel etkinliğini azaltmak amacıyla işbirliği yapmakta ve siber olaylara yanıt vermektedir. Üyeler siber tehdit bilgisi paylaşmakta, ortaklıklar kurmakta ve dijital ekosistemin genel güvenliğini ve dayanıklılığını artıran politikaları teşvik etmektedir. Bu kapsamda, üyeler Siber Tehdit İttifakı platformu üzerinden bilgi paylaşımının yanı sıra aynı zamanda Erken Paylaşım programı aracılığıyla araştırma bulgularını ve analizleri de paylaşmaktadır. Genel olarak Siber Tehdit İttifakı üyeleri haftada 3-4 erken paylaşım bilgisi almaktadır. Aralık 2019 ayında Siber Tehdit İttifakı tarafından yapılan ankette, katılımcıların büyük bir çoğunluğunun erken paylaşım programının üyeliğin önemli bir avantajı olduğunu vurgulamıştır. Paydaşlar tarafından gerçekleştirilen 300'den fazla erken paylaşım, siber tehditlere yönelik önlemlerin zamanında uygulanmasını sağlamış ve yeni siber güvenlik tehditlerinin daha fazla araştırılmasını kolaylaştırmıştır.

Ayrıca Siber Tehdit İttifakı platformu tarafından, CERT, ISAC, kar amacı gütmeyen emsal kuruluşlar ve Siber Tehdit İttifakı üyeliğine uygun olmayan diğer kuruluşlarla çeşitli ortaklıklar kurulmaktadır. Siber Tehdit İttifakı platformuna 2020 yılında OneFirewall, Anomali ve Security Scorecard olmak üzere 3 yeni paydaş eklenmiştir. Eylül ayında ise 100 milyon paylaşılan gözlemlenebilir tehdide ulaşıldığı ve Aralık ayında ise bu sayının 140 milyona ulaştığı vurgulanmaktadır. 2018 yılından beri diğer Siber Tehdit İttifakı üyeleriyle önceden paylaşılan 350'den fazla üye bloga ve tehdit raporuna ulaşılmıştır. 2020 yılında ayrıca "Finansal Hizmetler Bilgi Paylaşımı ve Analiz Merkezi (FS-ISAC)", "Bilgi

Teknolojileri ISAC", "CSIRT Asobancaria (Latin Amerika'daki finans kurumlarını temsil etmekte)", "Tayvan CERT" ve "İnternet Güvenliği Merkezi (CIS)" dahil olmak üzere katkıda bulunan beş müttefikle işbirliği kurulmuştur. Ayrıca Siber Tehdit İttifakı olarak "No More Ransom" girişimine katılım sağlanmıştır [63].

Ayrıca Siber Tehdit İttifakı platformundaki tehdit bilgisi birçok benzer kuruluştan çok daha zengin olup, gelecekteki paylaşımlar için veri iyileştirilmesi yapılmaktadır. Siber Tehdit İttifakı ayrıca kalite kontrolleri gerçekleştirmekte ve veriler hakkında platoformdan geri bildirim alınmaktadır. Platform üzerinden sağlanan verilerden 8.500 adet yeni örnek seçilmekte ve bunlar Siber Tehdit İttifakı üyelerine gönderilmektedir. Bu yeni örnekler düzenli olarak değerlendirilmekte ve üyelerin ihtiyaçları ile uyumlu olmaları sağlanmaktadır. İleriye dönük olarak ise Siber Tehdit İttifakı platformuna gönderilen meta verilerin zenginleştirilmesi için çalışmalar gerçekleştirilmektedir [64].

Siber Tehdit İttifakında ayırca siber güvenliği güçlendirmek amacıyla fidye yazılımı ve kötü amaçlı yazılımlar hakkında raporlar yayımlanmaktadır. Diğer paylaşım programlarının aksine Siber Tehdit İttifakı platformunda her üyenin bilgi paylaşması gerekmektedir. Her paydaşın, günde en az 1.000 parça benzersiz kötü amaçlı kod paylaşması gerekmekte ve platformda uyumluluğun sağlanması amacıyla üyelerden geri bildirim sağlanmaktadır.

Diğer taraftan, Siber Tehdit İttifakında tüm potansiyel üyeler kapsamlı bir inceleme sürecinden geçmekte, bu kapsamda tüm paydaşların ABD'de iş yapmaya uygun olmasının gerekmesi, platforma bilgi sağlamak için tüm üyelerin tehdit bilgisine sahip olmasının gerekmesi, tüm üyelerin tehdit bilgisini platformda paylaşma ve platformdan tedarik etme teknik kapasitesini koruması gerekmesi şartlarını yerine getirmesi gerekmektedir.

3.2. Avrupa Birliği Kamu Özel İşbirliği Modeli

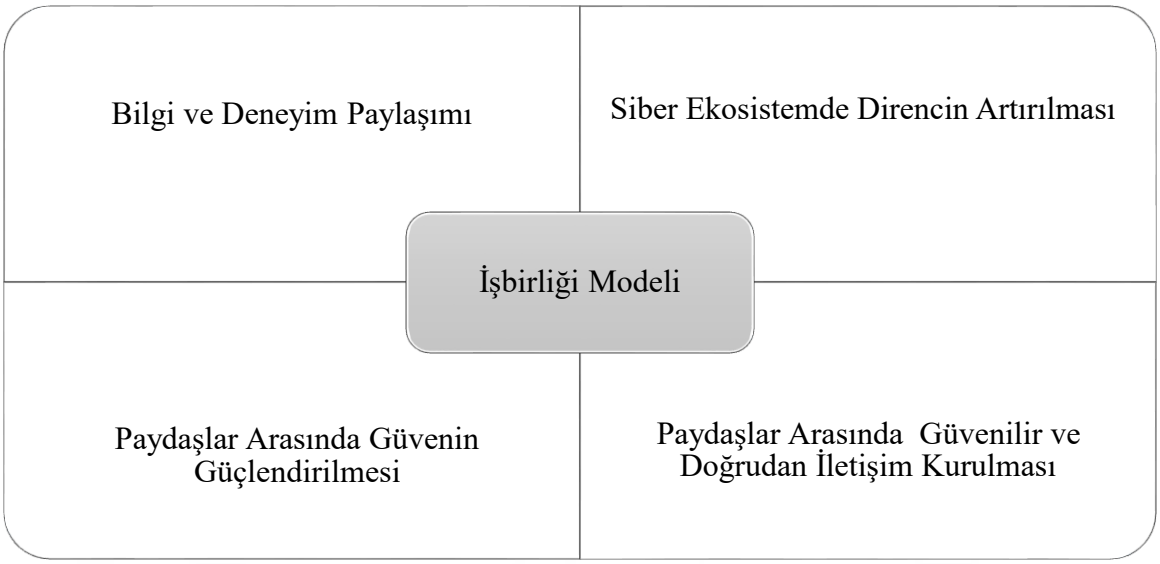
Siber tehditlerin doğru şekilde ele alınması için işbirliği, diyalog ve tüm paydaşların kapasitesinin geliştirilmesi önem teşkil etmektedir. Ulusal siber güvenlik stratejisinin ortak hedefi "işbirliği" olan AB'de ise siber güvenliği artırmak amacıyla işbirliği ile bilgi ve farkındalık oluşturma çalışmaları Bilgi Paylaşım ve Analiz Merkezleri (Information

Sharing and Analysis Center-ISAC) ve Kamu Özel Ortaklığı (PPP) aracılığıyla gerçekleştirilmektedir.

Bilgi Paylaşım ve Analiz Merkezleri, "siber tehditler hakkında bilgi toplamak için merkezi bir kaynak sağlayan ve özel ve kamu sektörü arasında iki yönlü bilgi paylaşımına izin veren kar amacı gütmeyen kuruluşlar" şeklinde tanımlanmaktadır. Birçok AB üye devletinde ISAC veya benzeri girişimler mevcut olup, söz konusu merkezler temel nedenler, olaylar ve tehditler hakkında bilgi paylaşımının yanı sıra deneyim, bilgi ve analiz paylaşımı açısından işbirliği için bir platform oluşturmaktadır. Havacılık, finans, enerji, sağlık ve denizcilik gibi alanlarda oluşturulan bilgi paylaşım merkezleri, Avrupa'da ilk olarak finans ve enerji sektöründe oluşturulmuştur [65].

AB'deki Kamu - Özel Ortaklığı ise iki veya daha fazla kamu ve özel sektör arasında uzun vadeli bir anlaşma, dayanışma ve işbirliği ortaklığı olarak tanımlanmaktadır [66]. ENISA tarafından 2017 yılından yayımlanan raporda; AB'de yer alan kamu özel sektör işbirliği modelinde 27 adet üye devletin bir işbirliği modeline sahip olduğu belirtilmektedir. Raporda AB'de; "Avusturya, Belçika, Bulgaristan, Hırvatistan, Çekya, GKRY, Danimarka, Estonya, Fransa, Finlandiya, Almanya, Yunanistan, Macaristan, İtalya, İrlanda, Litvanya, Letonya, Lüksemburg, Malta, Hollanda, Polonya, Portekiz, Romanya, Slovenya, Slovakya, İspanya ve İngiltere'de söz konusu işbirliği modelleri bulunduğu belirtilmektedir [66].

AB Kamu Özel Ortaklığında paydaşlar arasında deneyim paylaşımı ve güvenilir bağlantılar kurulması gibi çalışmalar hedeflenmiştir. Şekil 3.1'de AB Kamu Özel Ortaklığında hedeflenen çalışmalar belirtilmiştir.



Şekil 3.1. AB Kamu Özel Ortaklığı İşbirliği Modeli [66]

AB Kamu - Özel Ortaklığı işbirliği modelinde ayrıca;

- Paydaşlar arasında sinerji oluşturma imkanı sağlanabilmektedir.
- Paydaşlar tarafından desteklendiği için paylaşılan bilgilerin kaliteli ve verimli olduğuna dair güven sağlanabilmektedir.
- Bilgi, deneyim ve en iyi uygulamalar paydaşlarla paylaşılabilmektedir.
- Siber ekosistemde siber tehditlere yönelik direnç sağlamaya yardımcı olunmaktadır.
- Paydaşlar arasındaki güvenin artması, farklı paydaşlarla tanışmaya olanak tanınması ve bu sayede kriz anında daha iyi bilgi ve proaktif tutum elde edilmesi sağlanabilmektedir.
- Diğer paydaşlarla doğrudan ve güvenilir bağlantılar kurulabilmektedir.

Ayrıca bahse konu işbirliği modelinde özel sektör temsilcilerinin daha fazla bütçeye sahip olma imkânı bulması, kamunun sektördeki bilgi ve güveninden faydalanılması, işbirliği modelinde paylaşılan bilgilerin kaliteli olduğu konusunda güvenin sağlanması hususları, özel sektör temsilcililerini bu işbirliği modeline katılmaya teşvik etmektedir. İşbirliği mekanizmasının kamuya olan yararına bakıldığında ise, sektörün daha iyi anlaşılabilmesi, özel sektör paydaşları arasında sinerjinin oluşturulabilmesi ve özel sektör deneyimlerini ve tecrübelerinden faydalanılabilmesi konuları ön plana çıkmaktadır [66].

3.3. İngiltere Siber Güvenlik Bilgi Paylaşım Ortaklığı

İngiltere'de siber tehdit bilgisinin paylaşılması amacıyla Siber Güvenlik Bilgi Paylaşım Ortaklığı (CISP) faaliyet göstermektedir. 2013 yılında oluşturulan CISP, "siber tehdit bilgilerini gerçek zamanlı olarak, güvenli, gizli ve dinamik bir ortamda paylaşmak, durumsal farkındalığı artırmak ve İngiltere'deki iş dünyası üzerindeki etkisini azaltmak için kurulmuş ortak bir endüstri ve hükümet girişimi" olarak tanımlanmaktadır. CISP, sektörler ve kuruluşlardan üyelerin, güvenli ve dinamik bir ortamda gerçek zamanlı olarak siber tehdit bilgilerini paylaşmalarına olanak tanımaktadır [67].

CISP, geniş bir ürün yelpazesi üretmekte olup, söz konusu ürünler arasında; ulusal ve uluslararası ortaklar da dâhil olmak üzere siber tehditlere dair uyarılar ve öneriler, ortak temalara ilişkin en iyi uygulama ve rehberlik belgeleri, tehdit eğilimlerine ilişkin üç aylık raporlar, kötü amaçlı yazılım ve kimlik avı e-posta analizi bulunmaktadır [68].

Söz konusu girişim ile güvenli bir ortamda sektör ve kamu arasında etkileşim, siber tehditlere karşı erken uyarı sağlama, diğer kullanıcıların deneyimlerinden, hatalarından, başarılarından öğrenme ve tavsiye alma yeteneğinin kazanılması ve organizasyon ağlarını korumak için gelişmiş bir yetenek kazanılması amaçlanmaktadır.

CISP topluluğu, kuruluşların karşılaştığı en son siber güvenlik bilgilerini, haberleri ve tehditleri paylaşmak ve bunlarla ilgili işbirliği yapmak için güvenli, sınırlı erişimli bir çevrimiçi işbirliği ortamı kullanmaktadır. CISP platformunda katılımı teşvik etmek ve üyelerin hassas siber güvenlik bilgilerini paylaşmalarını kolaylaştırmak için anonimlik ve bir bilgi işleme modeli tanımlanmıştır.

Bilgi işleme modeli, içeriğin kırmızı, sarı, yeşil veya beyaz olarak işaretlenebildiği bir "trafik ışığı" protokolüne dayanmaktadır. Paydaşın paylaştığı bir bilgi parçasına atadığı renk, topluluktaki diğer üyelerin bilgileri nasıl daha fazla paylaşabileceğini tanımlamaktadır. Örneğin, kırmızı olarak işaretlenmiş bir bilgi, paydaşın paylaşmayı belirlediği paydaş grubunun dışında paylaşılamamakta iken yeşil olarak işaretlenmiş bir bilgi ise paydaşlar ile paylaşılabilmektedir [6].

2014 yılı itibarıyla 777 kuruluşun ve 2.223 kişinin topluluğa katıldığı CISP, İngiltere'de siber güvenlik uyarılarını çok sayıda kuruluşa hızlı ve etkili bir şekilde dağıtmanın bir yolu olarak da kullanılmaktadır [6].

3.4. Ülkemizdeki Siber Güvenlik Çalışmaları ve Ekosistemi

Ülkemizde siber güvenlik çalışmaları 2012 yılında hız kazanmaya başlamıştır. 11/6/2012 tarihli ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" başlıklı Bakanlar Kurulu Kararı ile Siber Güvenlik Kurulu kurulması kararlaştırılmıştır. Siber Güvenlik Kurulu'na "siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan plan, program ve rapor, usul, esas ve standartları onaylamak ve bunların uygulanması ve koordinasyonunun sağlanması" görevleri verilmiştir [69]. Bunun yanında, söz konusu Karar ile Ulaştırma ve Altyapı Bakanlığı'nın siber güvenlikle ilgili görevleri belirlenmiştir. Karar kapsamında; "siber güvenlikle ilgili politika, strateji ve eylem planı hazırlanması, bilgi ve veri güvenliğinin sağlanmasına yönelik usul ve esasların hazırlanması, farkındalık oluşturma ve eğitim çalışmalarının gerçekleştirilmesi" görevleri Ulaştırma ve Altyapı Bakanlığı'na verilmiştir [69].

Akabinde 06/02/2014 tarihinde yayımlanan 6518 sayılı kanun ile 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen ek fıkralar ile Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir.

Siber Güvenlik Kurulunca 2012 yılında gerçekleştirilen toplantıda ise "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiş ve Bakanlar Kurulu'nun 20/06/2013 tarihli ve 28683 sayılı kararı ile Resmi Gazetede yayımlanarak uygulamaya konulmuştur. "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" ile kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan hizmetlerin ve sistemlerin güvenliğinin sağlanması, kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanması hedeflenmiştir. Söz konusu eylem planında 29 alt eylem maddesine yer verilmiştir.

Ayrıca "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nda yer alan "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı eylem maddesi uyarınca,

ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde USOM kurulmuştur [70].

Türkiye'nin ikinci Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise 2016 yılında kabul edilmiştir. Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, "Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması", "Siber Suçlarla Mücadele", "Farkındalık ve İnsan Kaynağı Geliştirme", "Siber Güvenlik Ekosisteminin Geliştirilmesi" ve "Siber Güvenliğin Milli Güvenliğe Entegrasyonu" olmak üzere 5 ana hedeften oluşmaktadır.

Türkiye'de 2018 yılında yapılan değişiklikle birlikte Siber Güvenlik Kurulu Cumhurbaşkanlığı'na bağlanmış, ayrıca Dijital Dönüşüm Ofisi oluşturulmuştur. Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirme görevi verilen Dijital Dönüşüm Ofisi bünyesinde Siber Güvenlik Daire Başkanlığı kurulmuştur.

2019 yılında ise siber tehditlerin etkisiz kılınması ve kritik türdeki verilerin güvenliğinin sağlanması amacıyla "2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi" yayımlanmıştır. 21 ana maddeden oluşan Genelgede, kritik verilerin saklanmasından ağ güvenliğine, bulut depolama hizmetlerinden sosyal medya uygulamalarına, TEMPEST güvenliğinden mobil cihaz güvenliğine, kripto sistemlerinden güvenli yazılım geliştirmeye ve endüstriyel kontrol sistemlerinden e-posta sistemlerine kadar pek çok konuda tedbirler yer almaktadır.

Ayrıca Genelge kapsamında, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyelerini içeren "Bilgi ve İletişim Güvenliği Rehberi'nin hazırlanacağı ifadesi yer almaktadır. Bu kapsamda, Dijital Dönüşüm Ofisi tarafından Bilgi ve İletişim Güvenliği Rehberi hazırlanmış olup, 2020 yılında yayımlanmıştır. Söz konusu Rehberde, uygulama ve veri güvenliği, taşınabilir cihaz güvenliği, Nesnelerin İnterneti, kişisel veri güvenliği, anlık mesajlaşma güvenliği, bulut bilişim güvenliği, kritik altyapı güvenliği gibi pek çok konudaki tedbirler detaylandırılmıştır [71].

Son olarak ülkemizdeki 3. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı "Ulusal Siber Güvenlik Stratejisi (2020-2023)" Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanarak Aralık 2020 ayında yayımlanmıştır. Siber alandaki varlıkların siber tehditlerden korunması ve siber tehditlerin azaltılmasına yönelik çalışmaların gerçekleştirilmesi amacıyla hazırlanan eylem planı, "kritik altyapıların korunması ve mukavemetin artırılması, ulusal kapasitenin geliştirilmesi, organik siber güvenlik ağının oluşturulması, yeni nesil teknolojilerin güvenliği, siber suçlarla mücadele, yerli ve milli teknolojilerin geliştirilmesi ve desteklenmesi, siber güvenliğin milli güvenliğe entegrasyonu ve uluslararası işbirliğinin geliştirilmesi" olmak üzere 8 ana stratejik hedef doğrultusunda hazırlanmıştır [55].

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında; "kritik altyapıların siber güvenliğinin korunması, proaktif siber savunma anlayışının geliştirilmesi, siber suçların en aza indirgenmesi ve caydırıcılığın artırılması, siber olaylara hazırlık seviyelerinin artırılması, SOME ekiplerinin olgunluk seviyelerinin geliştirilmesi, siber güvenlik alanında en güncel teknolojik imkânlara sahip olunması, yerli ve milli teknolojik imkânların geliştirilmesi, yeni nesil teknolojilerin güvenliğinin sağlanması, siber güvenlik farkındalığının artırılması, kurum ve kuruluşlarda kurumsal bilgi güvenliği kültürünün oluşturulması, kurum ve kuruluşlar arasında veri paylaşımının güvenli şekilde sağlanması, kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalmasının sağlanması ve bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi" çalışmaları hedeflenmektedir [55].

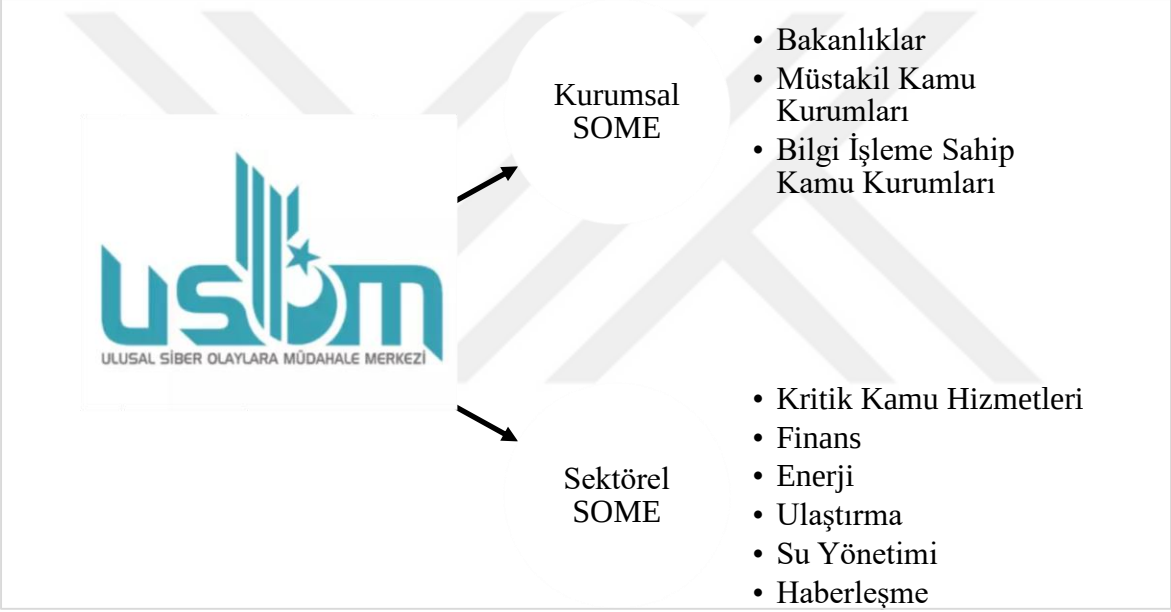
3.4.1. Ulusal Siber Olaylara Müdahale Merkezinin çalışmaları

Ülkemizde, kamu kurumları ve özel sektör arasında işbirliğinin sağlanması ve siber tehditlere yönelik hızlı aksiyon alınması, siber tehditlerin hedef alabileceği alanlarla hızlı koordinasyon kurulması ve işbirliği sağlanması amacıyla 2014 yılında USOM ve SOME ekipleri oluşturulmuştur. USOM, siber tehditleri önlemek amacıyla alarm, uyarı ve duyuru faaliyetleri yürütmekte, kritik durumlarda yerinde olaya müdahale etmektedir. USOM ayrıca siber güvenlik tehditlerine yönelik alarm, uyarı, duyuru faaliyetleri gerçekleştirmektedir.

Bunun yanı sıra, USOM bünyesinde faaliyet gösteren ve Kurumsal ve Sektörel olmak üzere 2 tür SOME oluşturulmuştur. Kurumsal SOME'ler "kurumlara doğrudan ya da

dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla" görevlendirilmiştir.

Kurumsal SOME'lerin Bakanlıklar ve Müstakil Kamu Kurumlarında faaliyet gösterdiği belirtilirken, Sektörel SOME'lerin ise finans, enerji, ulaşım, haberleşme vb. gibi kritik altyapı sektörlerinde faaliyet gösterdiği ifade edilmektedir. Şekil 3.2.'de Kurumsal ve Sektörel SOME'lerin faaliyet gösterdiği kuruluşlar belirtilmiştir.



Şekil 3.2. Ulusal Siber Olaylara Müdahale Merkezi organizasyonu [72]

USOM ile Kurumsal ve Sektörel SOME'ler arasında; uyarı ve bilgilendirmelerin paylaşılması, koordinasyon ve iletişim çalışmaları gerçekleştirilmektedir. Sektörel SOME'lerin siber olay öncesi/esnası/sonrasında olmak üzere çeşitli görevleri bulunmaktadır. Siber olay öncesinde; sektör içi siber güvenlik kriterlerinin belirlenmesi, sektörel siber olay müdahale prosedürünün oluşturulması, USOM tarafından yayımlanan duyuru ve bildirilerin sektöre aktarılması, siber saldırı uyarısı ve güvenlik açığı duyurusunun yayımlanması faaliyetleri icra edilmektedir.

Siber olay esnasında, kendisine bağlı olan Kurumsal SOME'lere ve USOM'a siber olayla ilgili bilgilendirme mesajı gönderilmesi, siber olay sonrasında ise; siber olay bildirim

formlarının Kurumsal SOME tarafından doldurulmasını, USOM'a iletilmesini sağlamakta, siber olaydan elde edilen, olayın önlenmesine yönelik bilgi ve tecrübelerin, sektördeki diğer Kurumsal SOME'ler ile paylaşılması çalışmalarını gerçekleştirilmektedir. Çizelge 3.3.'te USOM'un hizmet alanları belirtilmiştir.

Çizelge 3.3. USOM'un hizmet alanları [72]

Organizasyon	Kurulduğu Kurum/Kuruluş	Hizmet Alanı
USOM	BTK	Ulusal siber ortam
Sektörel SOME	Kritik sektörü düzenleyici ve denetleyici kurumlar Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili Bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Diğer taraftan, BTK tarafından 2017 yılında USOM ile SOME'ler arasında siber tehdit, zafiyet ve saldırıların güvenli/hızlı bir biçimde paylaşımını sağlayan SİP (SOME İletişim Platformu) Projesi hayata geçirilmiştir. Hâlihazırda 1.970 kayıtlı siber güvenlik uzmanı SİP sistemini kullanmakta olup, USOM'a kamu kurumları, uluslararası kuruluşlar, araştırma merkezleri ve üniversiteler, özel sektör gibi paydaşlardan ulaşan bildirimler ilgililere iletilerek gerekli tedbirlerin alınması sağlanmaktadır. USOM ayrıca "Forum of Incident Response Teams (FIRST)", "Trusted Introducers (TI)" ve "ITU-IMPACT" kuruluşlarına üyedir [73].

3.4.2. Siber güvenlik ekosistemi

2013-2014 ve 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında ülkemizde siber güvenlik ekosisteminin geliştirilmesine yönelik eylem maddeleri bulunmaktadır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında 14 ve 27 numaralı eylem maddelerinde kamu-özel sektör işbirliği konusuna değinilmiştir.

Bunun yanında, İnternet Geliştirme Kurulu bünyesinde sektörde yer alan bütün kurum ve kuruluşların katılım sağladığı Siber Güvenlik İnisiyatifi oluşturulmuştur. Bu çerçevede, bütün paydaşların görüşlerinin toplanması, kurumlar arası fikir alışverişi ve işbirliğinin sağlanması yoluyla ortak fikirler çıkarılması ve bu çalışmaların Ulaştırma ve Altyapı Bakanlığı'na sunulması hedeflenmektedir. Bu kapsamda; bilinçlendirmeyi artırma, farkındalık yaratma, koruma tedbirlerini oluşturma ve raporlar ve kılavuzlar yayımlanması faaliyetleri yürütülmektedir [74].

Ayrıca ülkemizde 2017 yılında siber güvenlik alanında işbirliğinin artırılması amacıyla Siber Güvenlik Kümelenmesi oluşturulmuştur. Türkiye Siber Güvenlik Kümelenmesi, 2017 yılında ülkemizde siber güvenlik ekosisteminin geliştirilmesi amacıyla ilgili tüm kamu kurum/kuruluşlar, özel sektör ve akademi temsilcilerinin katılımlarıyla kurulan ve Cumhurbaşkanlığı Savunma Sanayii Başkanlığı ve Dijital Dönüşüm Ofisi Başkanlığının desteği ve koordinasyonu ile yürütülen platform şeklinde tanımlanmaktadır. Siber güvenlik kümelenmesi, siber güvenlik alanında organizasyonların kümeler oluşturarak ortak hedefler doğrultusunda işbirliği yapması, farklı alanlarda faaliyet gösteren organizasyonların ortak paydada buluşmasını ifade etmektedir. İşbirliği modelinde benzer ilgi alanında olan organizasyonlar arasında bir iletişim ve etkileşim kurulması mümkün olabilmektedir [74].

Söz konusu Kümenin hedeflerinin belirlenmesi ve yönetilmesi Danışma Kurulu vasıtasıyla gerçekleştirilmektedir. Danışma Kurulu, Sanayi ve Teknoloji Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Dijital Dönüşüm Ofisi Başkanlığı ve Savunma Sanayi Başkanlığı üst düzey temsilcilerinin katılımıyla oluşturulmuştur. Kümelenmeye ülkemizde siber güvenlik alanında ürün/hizmet geliştiren firmalar üye olabilmektedir.

Bahse konu Küme, "pazara erişim, inovasyon, yeteneğe erişim, etkileşim ve teknolojik üstünlük" olmak üzere 5 ana hususta faaliyetlerini sürdürmektedir. Kümelenme ile; ülkemizdeki siber güvenlik firmalarının sayısının artırılması, siber güvenlik ekosisteminin standartlarının geliştirilmesi, üyelerin gelişimine destek olunması, üyelerin ürün ve hizmetlerinin markalaşmasına yardımcı olunması, üyelerinin ulusal ve küresel pazarda

rekabet gücünün artırılması, siber güvenlik alanındaki insan kaynağı sayısının artırılması, ve siber güvenlik bilincinin geliştirilmesinin hedeflendiği belirtilmektedir [75].

Kümelenme kapsamında; "paydaşlar arasında iletişimin artırılması amacıyla etkinlikler düzenlenmesi, üye firmaların ürün ve hizmetlerinin kataloglandırılması, yerli ürünler için teşvik mekanizmalarının oluşturulması, üyelerinin tanıtımının yapılması, eğitim, yarışma gibi etkinlikler düzenlenmesi, teknolojik ve sektörel haber ve bültenlerin paylaşımının yapılması, danışmanlık yapılması, teknoloji yol haritasının oluşturulması, ulusal/uluslararası konferans, eğitim, seminer vb. etkinlikler düzenlenmesi" çalışmaları yürütülmektedir [75].

Haziran 2020 ayı itibarıyla 150 üyesi bulunan Kümede, Türkiye'de yerli ürünlerin geliştirilmesinin artırılması ve yerli ürünlerin küresel ölçekte rekabet edebilecek düzeye gelebilmesi amacıyla çalışmalar yürütülmektedir. Bu kapsamda, üyelerin pazardaki faaliyetlerinin artırılması için üye firmaların tanıtımını artırmaya yönelik çalışmalar gerçekleştirilmekte ve çeşitli fuarlara katılım destekleri sağlanmaktadır. Ayrıca siber güvenlik ekosisteminin geliştirilmesi ve sektördeki tüm paydaşların katılımının sağlanması için çeşitli etkinlikler düzenlenmekte olup, ulusal ve uluslararası konferanslar ve zirveler ile sektörün birbiriyle ve farklı sektörlerle olan etkileşimi sağlanmaktadır. Kümelenme ile üyelerin müşterek hareket edebilmeleri için çeşitli çalışma grupları oluşturularak sektörün ilgi duyduğu alanlarda çalışmalar gerçekleştirilmektedir [75].

Sonuç itibarıyla, tehdit bilgisi paylaşımı konusunda ABD ve AB'de örnek işbirliği modelleri bulunmaktadır. Ülkemizde de siber güvenlik alanında işbirliğinin artırılmasına yönelik çeşitli çalışmalar gerçekleştirilmektedir. USOM aracılığıyla tehdit bilgilerinin paylaşımı gerçekleştirilirken, Siber Güvenlik Kümelenmesinde ise ülkemizdeki siber güvenlik firmaları arasında işbirliği yapılarak firmaların ürünlerinin markalaşmasına yardımcı olunmaktadır.

Ayrıca ülkemizde tehdit bilgisi paylaşımı konusunda da çeşitli çalışmalar gerçekleştirilmekte olup, Ulusal Siber Güvenlik Stratejisi ve Eylem Planları, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde bu çalışmalara değinilmiştir. Çalışmanın 4. Bölümünde bu çalışmalar analiz edilerek önerilerde bulunulmuştur.

4. TÜRKİYE'DE TEHDİT BİLGİSİ PAYLAŞIM ÇALIŞMALARI VE DEĞERLENDİRMELER

Ülkemizde siber tehditlerle etkin bir şekilde mücadele edilebilmesi amacıyla tehdit bilgilerinin diğer paydaşlarla paylaşılmasına yönelik çeşitli çalışmalar gerçekleştirilmektedir. Ülkemizde siber güvenlik çalışmaları kapsamında hâlihazırda 3 adet Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmıştır. Ayrıca Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberi hazırlanarak yayımlanmıştır. Bu çalışmalar kapsamında ülkemizde siber tehdit bilgilerinin paylaşılmasına yönelik çeşitli hükümler yer almaktadır. Eylem planları kapsamında ülkemizde siber güvenlik ekosisteminin oluşturulmasına yönelik hususlara yer verilmektedir. Genelge ve Rehberde ise USOM tarafından yayımlanan bildirimler doğrultusunda ilgili kuruluşların gerekli tedbirleri alması gerekmektedir.

Bu bölümde, ülkemizde yayımlanan Ulusal Siber Güvenlik Stratejileri ve Eylem Planları ile birlikte Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberi, tehdit bilgisi paylaşımı kapsamında incelenmiştir. Eylem Planları, Genelge ve Rehbere ilişkin Zack Bilgi Boşluğu ve Maslow'un İhtiyaçlar Hiyerarşisi analizleri gerçekleştirilmiştir. Zack Bilgi Boşluğu analizi gerçekleştirilerek Eylem Planları, Genelge ve Rehberde tehdit bilgisi paylaşımı konusundaki stratejik boşluklar belirlenmiştir. Bu kapsamda, Eylem Planları, Genelge ve Rehberde; bilgi paylaşımı konusunda yer verilen hususlar, yer verilen hususlar ile neler yapılabileceği, yer verilmesi gerekilen hususlar ve yer verilmesi halinde neler yapılması gerekilen hususlar ele alınmıştır. Maslow Hiyerarşisi analizinde ise Eylem Planları, Genelge ve Rehberde tehdit bilgisi paylaşımı konusunda yer verilmesi gerekilen çalışmalar belirlenmiştir.

4.1. Bilgi ve İletişim Güvenliği Genelgesi ile Rehberinin İncelenmesi

Ülkemizde siber ortamdaki risklerin bertaraf edilmesi ve kritik verilerin güvenliğinin sağlanması amacıyla 2019 yılında "Bilgi ve İletişim Güvenliği Tedbirleri" başlıklı Genelge hazırlanmış olup, 06/07/2019 tarihli ve 30823 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. 21 maddeden oluşan Genelgede; kritik verilerin depolanması, mobil uygulamalar ve sosyal medya üzerinden gizlilik dereceli haberleşme ve veri paylaşımı yapılmaması, yerli uygulamaların tercih edilmesi, TEMPEST güvenliği, yerli ve milli

kripto sistemlerinin geliştirilmesi ve kullanılması, güvenli yazılım geliştirilmesi, siber tehdit bildirimleri ile ilgili gerekli tedbirlerin alınması, endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması, kamu e-posta sistemlerinin güvenli olacak şekilde yapılandırılması, yurt içinde değiştirilmesi gereken yurt içi iletişim trafiğinin yurt dışına çıkarılmaması ve kritik veri iletişiminde radyolink haberleşmesinin kullanılmamasına ilişkin tedbirler yer almaktadır.

Genelgede ayrıca siber tehdit bildirimlerine ilişkin 14 nolu "Kurum ve kuruluşlar siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır." maddesine yer verilmiştir [76]. Ancak bu madde haricinde siber tehdit bildirimleri ve bu bildirimlerin paylaşılmasına yönelik maddeye yer verilmemiştir. Bu madde kapsamında kurum ve kuruluşlardan, USOM tarafından paylaşılan bildirimleri ve tehdit raporlarında yer alan siber tehdit bildirimlerini takip etmeleri ve bu bildirimlere yönelik gerekli tedbirleri almasının beklendiği değerlendirilmektedir.

Ayrıca Genelge kapsamında, kurum ve kuruluşlar ve kritik altyapı işletmecilerinde uygulanmak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda "Bilgi ve İletişim Güvenliği Rehberi" hazırlanacağı belirtilmiştir. Bu çerçevede, "Bilgi ve İletişim Güvenliği Tedbirleri" konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi kapsamında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda paydaşların katılımıyla Bilgi ve İletişim Güvenliği Rehberi hazırlanmış ve 2020 yılında yayımlanmıştır.

Bilgi güvenliği risklerinin azaltılması ve kritik verilerin güvenliğinin sağlanması amacıyla asgari güvenlik tedbirlerinin belirlenmesi ve bu tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması amacıyla hazırlanan Rehberde; "ağ ve sistem güvenliği, uygulama ve veri güvenliği, taşınabilir cihaz ve ortam güvenliği, Nesnelerin İnterneti cihazlarının güvenliği, personel güvenliği, fiziksel mekânların güvenliği, kişisel verilerin güvenliği, anlık mesajlaşma güvenliği, bulut bilişim güvenliği, kripto uygulamalarının güvenliği ve sıkılaştırma tedbirleri" konu başlıklarındaki teknik tedbirlere yer verilmiştir [76].

Rehberde ayrıca siber tehdit bildirimlerine ilişkin hususlara "Ağ ve Sistem Güvenliği" başlığı altındaki "Siber Güvenlik Olay Yönetimi" başlığında değinilmiştir. Bu başlık altında; siber olaylara müdahale planlarının hazırlanması, siber olay yönetimi

kapsamında görev alacak personelin belirlenmesi, siber tehdit bildirimlerinin yönetilmesi, siber olayların raporlarının standardize edilmesi ve yayınlanması, üçüncü taraflardan alınan siber olay yönetim hizmetleri, SOME personeli için periyodik siber olay tatbikatlarının yapılması ve siber olay yönetimi puanlama ve önceliklendirme başlıkları olmak üzere alınması gereken 8 adet siber güvenlik tedbiri belirlenmiştir.

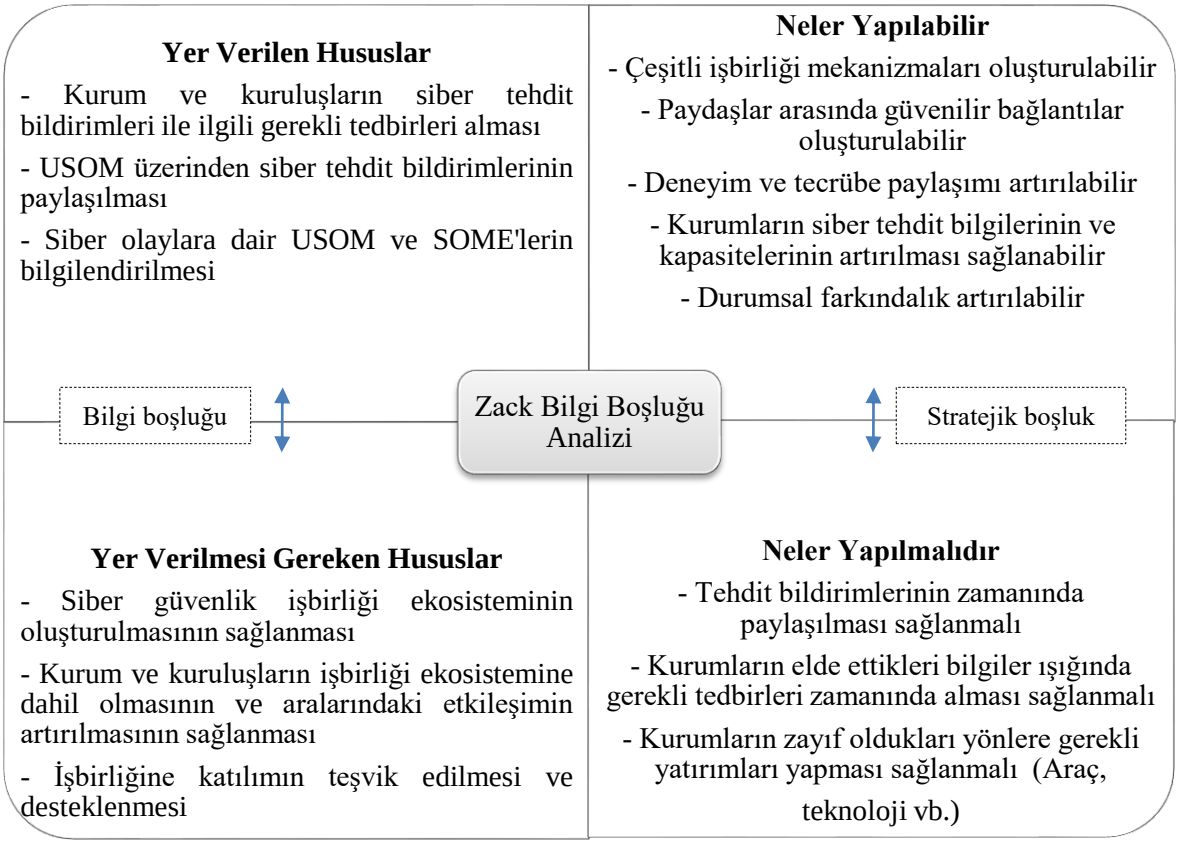
"Siber Tehdit Bildirimlerinin Yönetilmesi" maddesinde kurumlardan, siber olayların tespiti için gerekli altyapıları oluşturması ve USOM ve diğer siber tehdit istihbarat kaynaklarından temin edilen bildirimler doğrultusunda gerekli önlemleri alması beklenmektedir. "Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması" maddesinde ise siber olayların kuruma potansiyel etkileri göz önünde bulundurularak puanlanması ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme için risk temelli bir model kullanılması gerektiği belirtilmektedir.

Bilgi ve İletişim Güvenliği Rehberinde siber tehdit bilgilerinin paylaşılması konusunda ise USOM tarafından kurumlara siber tehdit bildirimlerinin iletileceği, kurumların bu bilgiler doğrultusunda önlem alacağı ve kurum/kuruluşların yaşanan siber olayları USOM'a ve Sektörel SOME'lere bildireceği hususlarına değinilmiştir. Bu çerçevede, siber tehdit bilgilerinin paylaşılmasına yönelik USOM üzerinden bilgi paylaşımı yapılacağı, kurumların ise yaşanan siber olaylara dair bildirimde bulunacağı anlaşılmaktadır.

Bu çerçevede, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberi incelendiğinde, siber tehdit bilgilerinin paylaşılmasına yönelik çalışmaların detaylarına yer verilmediği, yalnızca USOM üzerinden paylaşılan siber tehdit bildirimlerine değinildiği değerlendirilmektedir.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde yer verilen hususlar, yer verilmesi gereken hususlar, yer verilen hususlar ile neler yapılabileceği ve neler yapılması gerekildiği hususlarının belirlenebilmesi ve bu konudaki stratejik boşluğun belirlenerek giderilebilmesi amacıyla Zack Bilgi Boşluğu analizinden yararlanılmıştır. Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde siber tehdit bilgilerine yönelik bilgi paylaşımı konusunda yer verilmesi gerekilen hususların belirlenebilmesi için ise Maslow Hiyerarşisinden yararlanılmıştır.

Şekil 4.1.'de Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde tehdit bilgisi paylaşımı konusundaki bilgi boşluklarının ve stratejik boşlukların giderilmesi için gerçekleştirilmesi gerekilen çalışmalar belirtilmiştir.

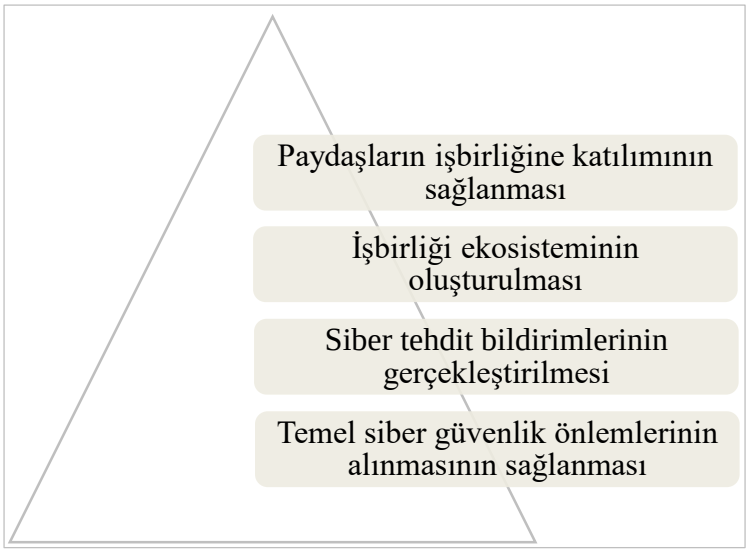


Şekil 4.1. Genelge ve Rehberin Zack Bilgi Boşluğu yaklaşımı açısından analizi

Analiz neticesinde, Genelgede ve Rehberde siber tehdit bilgilerinin paylaşılmasına yönelik işbirliği konusunun detaylıca ele alınmadığı, bu konuda stratejik boşlukların bulunduğu değerlendirilmiştir. Zack Bilgi Boşluğu analizinde belirlenen bilgi boşluğunun doldurulabilmesi için ülkemizde siber güvenlik işbirliği ekosisteminin oluşturulmasının sağlanması, paydaşların bu ekosisteme dâhil olmasının sağlanması, işbirliğine katılımın teşvik edilmesi ve paydaşlar arasında etkileşimin artırılmasının sağlanmasına yönelik hususların Genelge ve Rehberde yer verilebileceği değerlendirilmektedir. Bu çalışmaların yapılması ile birlikte, kurumların siber tehdit bilgilerinin ve kapasitelerinin artırılmasının sağlanabileceği, çeşitli işbirliği mekanizmalarının oluşturulabileceği, bu sayede deneyim ve tecrübe paylaşımının artırılabileceği, paydaşlar arasında güvenilir bağlantılar oluşturulabileceği ve durumsal farkındalığın artırılabileceği düşünülmektedir. Siber güvenlik işbirliği mekanizmalarının oluşturulması halinde ise paydaşlar tarafından tehdit

bildirimlerinin zamanında paylaşılması, paydaşların elde ettikleri bilgiler ışığında gerekli tedbirleri zamanında alması, kurumların zayıf oldukları yönlere gerekli altyapı, teknoloji, personel vb. gerekli yatırımları yapması gerekmektedir. Bu sayede paydaşların siber güvenlik kapasitesinin artacağı ve paydaşların işbirliği sayesinde yeni savunma stratejileri geliştirebileceği düşünülmektedir. Böylelikle Zack Bilgi Boşluğundaki stratejik boşluğun doldurulabilmesi mümkün olabilecektir.

Bilgi ve İletişim Güvenliği Genelgesi ve Rehberine ilişkin Maslow Hiyerarşisi analizi gerçekleştirildiğinde ise; Rehberde ve Genelgede öncelikli olarak kurum ve kuruluşların temel siber güvenlik önlemlerini almasının sağlanmasına yer verilmesi gerektiği değerlendirilmektedir. İkinci basamakta ise USOM'un tehdit bildirimlerini kuruluşlarla paylaşması, kuruluşların ise yaşanan siber olayları ve tespit ettikleri tehdit bilgilerini USOM ile paylaşması gerektiği değerlendirilmektedir. Üçüncü aşamada ise siber güvenlik işbirliği ağının genişletilmesi, spesifik bilgi paylaşım mekanizmalarının oluşturulması gerektiği, son basamakta ise paydaşların bu işbirliği mekanizmalarına katılmasının sağlanması gerektiği değerlendirilmektedir. Şekil 4.2.'de Maslow'un Hiyerarşisi analizi kapsamında Genelge ve Rehberde yer verilmesi gerekilen hususlar belirtilmiştir.



Şekil 4.2. Genelge ve Rehberin Maslow Hiyerarşisi yaklaşımı açısından analizi

Maslow Hiyerarşisi kapsamında ele alınan basamaklardan ilk iki basamaktaki hususlara Genelgede ve Rehberde yer verildiği görülmektedir. Bunun yanında, Maslow Hiyerarşisi kapsamında ele alınan son iki basamaktaki hususlara ise Genelgede ve Rehberde yer verilmediği, bu kapsamda ülkemizde işbirliği ekosisteminin oluşturulması ve paydaşların

da bu işbirliğine katılımının sağlanmasına yönelik çalışmaların gerçekleştirilmesinin, Siber Vatandaki varlıkların korunabilmesi ve kurum ve kuruluşların siber güvenlik kapasitesinin artırılabilmesine büyük katkı sağlayacağı değerlendirilmektedir.

4.2. Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının İncelenmesi

Ülkemizde Ulaştırma ve Altyapı Bakanlığı tarafından 2013-2014, 2016-2019 ve 2020-2023 dönemlerine yönelik Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanmıştır. 2013-2014 dönemi Ulusal Siber Güvenlik Stratejisi ve Eylem Planında USOM'un kurulması ve Sektörel ve Kurumsal SOME ekiplerinin oluşturulması maddelerine yer verilmiş ve USOM kurulmuştur. Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planında ise "Siber Güvenlik Ekosisteminin Geliştirilmesi" maddesine yer verilmiştir. Bu eylem maddesi kapsamında ise kamu, özel sektör, sivil toplum kuruluşları ve diğer paydaşların koordineli katkısıyla gereksinimlerin belirlenmesi ve uygulamaya konulmasına ilişkin çalışmaların gerçekleştirilmesi hedeflenmiştir. Ayrıca ulusal siber güvenlik ekosistemi içerisinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması amaçlanmıştır.

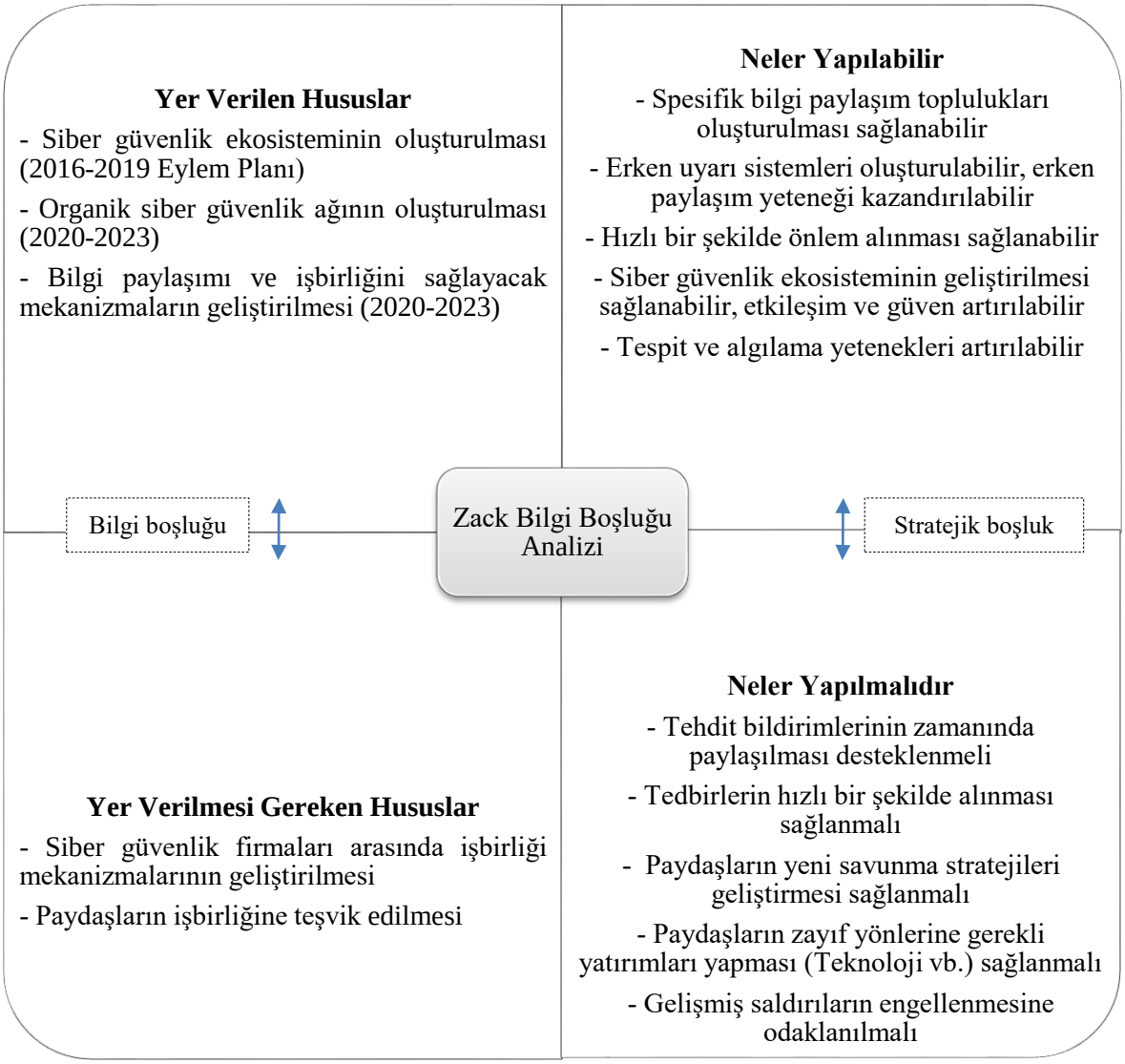
2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bütünsel bir süreç olduğu belirtilerek proaktif siber savunma anlayışının geliştirilmesi gerektiği belirtilmektedir. Ayrıca ulusal güvenliği tehdit edici bir unsur olan siber tehditlerin tespitinin zorlaştığı ve bu tehditlere karşı koymak için tehditlerin analiz edilmesi ve güvenlik ekiplerinin yetkinliklerinin geliştirilmesi gerektiği vurgulanmaktadır. Bu kapsamda, ülkemizde siber güvenlik alanında çalışanların bilgi ve tecrübe paylaşımına katılmasına olanak tanıyacak işbirliği çalışmalarının geliştirilmesi amacıyla 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında "Organik Siber Güvenlik Ağının Geliştirilmesi" maddesine yer verilmiştir. Bu madde kapsamında, siber saldırı yöntemlerine yönelik bilgilerin tek bir kaynaktan temin edilmesinin mümkün olmaması sebebiyle siber güvenlikte kaynakların çeşitlenmesi gerektiği belirtilmektedir. Bu kapsamda ülkemizde, ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi sağlanarak USOM ve SOME'lerin kapasitelerinin artırılması ve USOM'un paydaşları ile olan bilgi alışverişinin ve etkileşiminin geliştirilmesi amaçlanmaktadır [55].

2013-2014, 2016-2019 ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planları incelendiğinde ise 2016-2019 dönemi için hazırlanan eylem planında genel çerçevede siber güvenlik ekosisteminin oluşturulmasına değinildiği, 2020-2023 dönemi için hazırlanan eylem planında ise ülkemizde paydaşlarla bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi amacıyla çalışmalar gerçekleştirileceği ve USOM'un paydaşları ile bilgi alışverişinin ve etkileşiminin geliştirileceği vurgulanmaktadır. Siber tehdit bildirimlerinin paylaşılmasına yönelik işbirliği mekanizmalarının oluşturulması hususu önceki eylem planlarında yer almazken, 2020-2023 dönemi için hazırlanan eylem planında bu konuya yer verilmiştir. Ancak bu konuda belirtilen eylem maddesine ait alt eylem maddelerine ve uygulama adımlarına ise yer verilmemiştir.

Eylem planlarında yer verilen hususlar, yer verilmesi gereken hususlar, yer verilen hususlar ile neler yapılabileceği ve neler yapılması gerekildiği hususlarının belirlenebilmesi ve bu konudaki stratejik boşluğun belirlenerek giderilebilmesi amacıyla Zack Bilgi Boşluğu analizinden yararlanılmıştır. Ayrıca eylem planlarında siber tehdit bilgilerine yönelik bilgi paylaşımı konusunda yer verilmesi gerekilen hususların belirlenebilmesi için ise Maslow Hiyerarşisinden yararlanılmıştır.

Bu kapsamda, eylem planlarına ilişkin Zack Bilgi Boşluğu analizi gerçekleştirildiğinde, daha önce Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberine yönelik gerçekleştirilen Zack Bilgi Boşluğu analizinde belirlenen bilgi boşluğunun, 2020-2023 eylem planına eklenen "Organik siber güvenlik ağının oluşturulması" maddesi ile giderildiği, bunun yanında bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi maddesi ile stratejik boşluğunun da giderilmesine yönelik çalışmalara yer verildiği değerlendirilmektedir.

Şekil 4.3.'te Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında tehdit bilgisi paylaşımı konusundaki bilgi boşluklarının ve stratejik boşlukların giderilmesi için gerçekleştirilmesi gerekilen çalışmalar belirtilmiştir.



Şekil 4.3. Siber Güvenlik Eylem Planlarının Zack Bilgi Boşluğu analizi

Eylem planlarında organik siber güvenlik ağının oluşturulması ile bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi hususlarına yer verilmektedir. Bunun yanında, ülkemizde siber tehdit bilgilerinin paylaşılmasına yönelik işbirliği çalışmalarının genişletilmesi ve yapılan çalışmalar ile yapılması gereken çalışmalar arasındaki boşluğun giderilebilmesi amacıyla 2020-2023 eylem planında siber güvenlik firmaları arasında işbirliği mekanizmalarının geliştirilmesi, paydaşların işbirliğine teşvik edilmesi, işbirliği için gerekli altyapıların oluşturulmasına yönelik maddelerin eklenebileceği değerlendirilmektedir. Böylelikle Siber Vatanda spesifik bilgi paylaşım topluluklarının oluşturulabileceği, erken uyarı sistemlerinin oluşturulabileceği, tehditlere yönelik erken paylaşım yeteneği kazanılabileceği, siber tehditlere yönelik hızlı bir şekilde önlem alınabileceği, siber güvenlik ekosisteminin geliştirilmesinin sağlanabileceği, etkileşim ve

güvenin artırılabileceği, paydaşların kendi kapasitelerini artıracak çalışmalar gerçekleştirmesinin sağlanabileceği düşünülmektedir. Eylem planlarında yer verilmesi gereken hususlar kısmında ise siber tehdit bildirimlerinin zamanında paylaşılmasının sağlanması, gerekli tedbirlerin hızlı bir şekilde alınmasının sağlanması, paydaşların yeni savunma tedbirleri geliştirmesinin sağlanması, paydaşların gelişmiş saldırıların tespitine odaklanmasının sağlanması ve paydaşların savunma politikalarına ve zayıf yönlerine yönelik gerekli yatırımları yapmasının (Araç, teknoloji vb.) sağlanması hususlarının yer alması gerektiği değerlendirilmektedir. Böylelikle, paydaşların gelişmiş siber tehditleri engellemeye yönelik kapasitelerini geliştirebileceği ve siber tehdit bilgilerinin elde edilmesine yönelik organizasyonlardaki stratejik boşluğun doldurulabileceği değerlendirilmektedir.

Eylem planlarına ilişkin Maslow'un İhtiyaçlar Hiyerarşisi analizi gerçekleştirildiğinde ise; eylem planlarında siber güvenlik alanında işbirliğinin geliştirilmesi amacıyla öncelikle siber güvenlik ekosisteminin oluşturulması gerektiği değerlendirilmektedir. Sonraki aşamada ise siber tehdit bilgilerinin paylaşılmasına yönelik işbirliği mekanizmalarının oluşturulması gerektiği değerlendirilmektedir. Son aşamada ise Siber Vatanda paydaşlar arasında etkileşimin artırılması ve siber güvenlik direncinin artırılması amacıyla spesifik işbirliği mekanizmalarının oluşturulması gerektiği değerlendirilmektedir. Şekil 4.4.'te Maslow'un Hiyerarşisi analizi kapsamında Eylem Planlarında yer verilmesi gerekilen hususlar belirtilmiştir.

Şekil 4.4. Siber Güvenlik Eylem Planlarının Maslow Hiyerarşisi analizi

2020-2023 Ulusal Siber güvenlik Stratejisi ve Eylem Planında işbirliği mekanizmalarının oluşturulmasına yönelik yer verilen hususlar ile Maslow Hiyerarşisinin ilk iki basamağındaki çalışmalara yer verildiği değerlendirilmekte olup, bu kapsamda hiyerarşinin son basamağında yer alan spesifik işbirliği mekanizmalarının oluşturulmasına yönelik çalışmaların gerçekleştirilmesi gerektiği değerlendirilmektedir.

4.3. Değerlendirmeler

Siber tehdit bilgisi, siber tehditlerin tespit edilmesi, değerlendirilmesi, izlenmesi ve bu tehditlerle mücadele edilebilmesi noktasında organizasyonlara yardımcı olmaktadır. Bilgi paylaşımı yapan organizasyonlar;

- Kendi güvenlik seviyelerini artırdığı gibi diğer organizasyonların güvenlik seviyelerini de artırmaktadır.
- Karşı karşıya kalınan siber tehditleri daha kapsamlı anlayabilmesi için bilgi paylaşımı topluluğunun bilgisinden, deneyimlerinden ve kapasitelerinden yararlanmalıdır.
- Diğer paydaşların bilgisinden faydalanarak güvenlik seviyelerini artırmaktadır.
- Savunma yeteneklerini artırmakta, paylaşılan bilgileri kullanarak etkilenen sistemleri tanımlayabilmekte, koruyucu önlemler alabilmekte, algılama yeteneklerini geliştirebilmekte ve tehdit ortamındaki gözlenen değişikliklere dayanarak olaylara daha etkili bir şekilde müdahale edebilmekte, mevcut bilginin olgunlaşmasına yardımcı olmakta, mevcut bilgiler, paylaşılan bilgiler ile ilişkilendirilebilmekte ve bilginin değeri artabilmekte ve tehditleri hızlı bir şekilde tespit edebilmektedir.

Ülkemizdeki durum genel olarak değerlendirildiğinde ise;

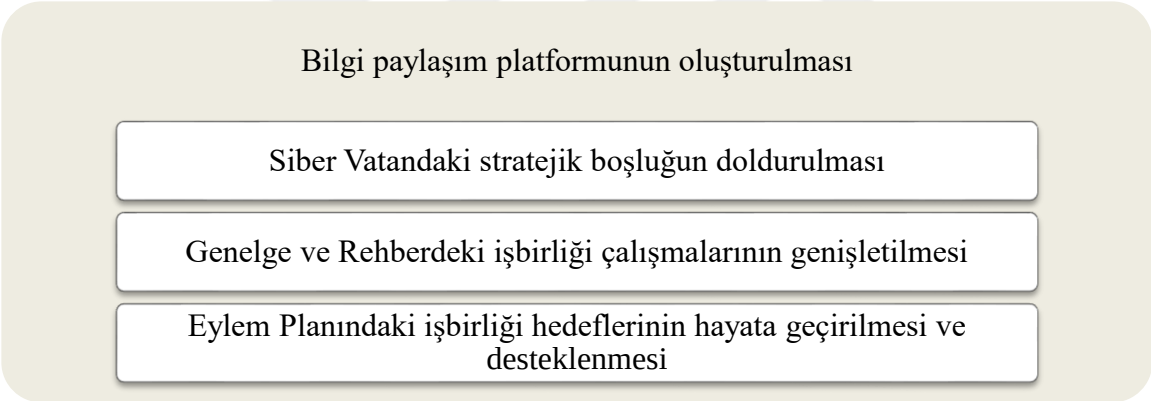
- Siber güvenlik alanındaki işbirliğini geliştirmeye yönelik çeşitli çalışmalar yürütülmektedir.
- Siber güvenlik ekosisteminin geliştirilmesi amacıyla gerçekleştirilen çalışmalarından biri olan Siber Güvenlik Kümelenmesinde ülkemizdeki siber güvenlik firmalarının sayısının artırılması, üyelerinin gelişimine destek olunması, bu alandaki insan kaynağı sayısının artırılması ve siber güvenlik bilincinin geliştirilmesi hedeflenmektedir.

- 2019 ve 2020 yıllarında yayımlanan Bilgi ve İletişim Güvenliği Genelgesi ve Rehberinde, siber tehdit bilgilerinin paylaşılmasına yönelik bir işbirliği mekanizması oluşturulması konusuna yer verilmemiştir.
- 2013-2014, 2016-2019 ve 2020-2023 dönemleri için hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında ise siber güvenlik ekosisteminin oluşturulması, ülkemizdeki bilgi ve tecrübe paylaşımına imkân verecek işbirliği çalışmalarının geliştirilmesi ve bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi hususlarına yer verilmiş olup, bu maddelere dair alt eylem maddeleri ve uygulama adımlarına ise değinilmemiştir.
- 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planına kadar eylem planlarında yer verilmeyen tehdit bilgilerinin paylaşılmasına yönelik işbirliği mekanizmalarının geliştirilmesi hususuna ise bu eylem planında yer verilmiş, ancak konuya ilişkin detaylara değinilmemiştir.
- Gerçekleştirilen incelemelerde, ülkemizde tehdit bilgilerinin paylaşılmasına yönelik işbirliği mekanizmalarının oluşturulmasına ilişkin çalışmalara, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde yer verilmemiş olup, yalnızca 2020-2023 eylem planında yer verilmiştir. Eylem planında yer verilen bu çalışmaların ise henüz uygulamaya konulmadığı değerlendirilmektedir. Ülkemizde tehdit bilgisi paylaşımına yönelik işbirliği mekanizması oluşturulması konusunda stratejik boşlukların bulunduğu düşünülmektedir.
- Nitekim Siber Vatanda yapılan çalışmalara yönelik gerçekleştirilen Zack Bilgi Boşluğu analizinde tehdit bilgilerine yönelik bilgi paylaşımı konusunda stratejik boşluk bulunduğu belirlenmiştir. Maslow Hiyerarşisi analizi neticesinde ise Siber Vatanda işbirliği çalışmalarının artırılması gerektiği değerlendirilmiştir.
- Bilgi ve İletişim Güvenliği Genelgesi ve Rehberine ilişkin Zack Bilgi Boşluğu analizi ve Maslow Hiyerarşisi incelendiğinde ise Genelgede ve Rehberde, ülkemizde siber güvenlik işbirliği ekosisteminin oluşturulmasının sağlanması ve paydaşların bu işbirliğine katılımının sağlanmasına yönelik çalışmalara yer verilmesi gerektiği değerlendirilmiştir.
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarına ilişkin Zack Bilgi Boşluğu analizi ve Maslow Hiyerarşisi incelendiğinde ise 2020-2023 eylem planında, Genelge ve Rehberde belirlenen stratejik boşlukların giderildiği, ancak bu çalışmaların henüz uygulamaya konulmadığı, bu kapsamda 2020-2023 dönemi eylem planında spesifik

işbirliği mekanizmalarının oluşturulmasına yönelik maddelere yer verilmesi gerektiği değerlendirilmiştir.

- Sonuç olarak, ülkemizde bilgi paylaşım mekanizmalarının oluşturulması konusundaki eksikliklerin giderilmesi, bu yöndeki çalışmaların artırılması ve Siber Vatanda işbirliği konusundaki farkındalığın ve paylaşım kültürünün geliştirilmesi gerektiği değerlendirilmektedir.
- Bu kapsamda, ülkemizde tehdit bilgilerinin hızlı bir şekilde paylaşıldığı, paydaşların birbirleriyle etkileşime geçebildiği, diğer paydaşların bilgi ve deneyimlerinden faydalanabildiği ve geniş yelpazede organizasyonun katılım sağladığı işbirliği mekanizmalarının geliştirilmesi gerektiği değerlendirilmektedir.

Şekil 4.5.'te, ülkemizde oluşturulması önerilen bilgi paylaşım platformunun gerekçeleri belirtilmiştir.



Şekil 4.5. İşbirliği mekanizmasının oluşturulmasının gerekçeleri

Sonuç olarak;

- Siber Vatanda siber tehditlere ilişkin bilgi paylaşımı konusundaki stratejik boşluğun doldurulabilmesi, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberinde genişletilmesi gereken bilgi paylaşımı konusunun genişletilebilmesi, 2020-2023 dönemi eylem planı kapsamında hedeflenen işbirliği mekanizmaları oluşturulmasına ilişkin çalışmaların hayata geçirilmesi ve bu konudaki çalışmalara katkı sunabilmesi amacıyla ülkemizde siber güvenlik firmaları arasında bilgi paylaşımına imkân tanıyacak işbirliği platformunun oluşturulması önerilmektedir.

- Ülkemizde de ABD ve AB'deki mekanizmalara benzer şekilde siber güvenlik firmaları arasında işbirliği platformunun oluşturulmasının, Siber Vatanın siber güvenliğinin sağlanması ve Siber Vatandaki her paydaşın siber güvenlik kapasitesinin artması açısından faydalı olacağı düşünülmektedir.
- Önerilen bilgi paylaşım platformu ile Siber Vatanda, Genelge ve Rehberde ve Eylem Planlarında belirlenen işbirliği mekanizması oluşturulması noktasındaki stratejik boşlukların giderilebileceği değerlendirilmektedir.
- Ayrıca 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında yer alan bilgi paylaşımı ve işbirliğini sağlayacak mekanizmaların geliştirilmesi konusundaki çalışmaların hayata geçirileceği ve bu çalışmalara katkı sağlanacağı düşünülmektedir.

5. ORGANİZASYONLAR İÇİN ANALİZ VE DEĞERLENDİRMELER

Siber uzayda meydana gelen ve gizlilik ihlaline neden olabilen sofistike tehditler, organizasyonların karşılaştığı en büyük zorlukların başında gelmektedir. Organizasyonların bu tehditlerle mücadele edebilmesi için bu tehditleri tanıması ve bu kapsamda önlem alması gerekmektedir. Siber tehdit bilgileri, siber tehditlerle mücadelede organizasyonlara büyük katkı sağlamakta, tehditlerin anlaşılmasına ve saldırganların davranışlarının belirlenmesine yardımcı olmaktadır.

Ancak, siber saldırganların yapısının anlaşılabilmesi, siber varlıkların daha iyi korunabilmesi ve yeni savunma stratejilerinin ve yaklaşımlarının geliştirilebilmesi için tehditler hakkında daha fazla bilgi edinilmesi gerekmektedir. Bu bağlamda, siber uzayda işbirliği çalışmalarının gerçekleştirilmesi ve diğer paydaşların bilgi ve tecrübelerinden faydalanılması gerekmektedir. Bu kapsamda ülkemizde tehdit bilgilerinin paylaşılması amacıyla siber güvenlik şirketleri arasında bilgi paylaşım platformunun oluşturulması önerilmiştir.

Bu kapsamda, organizasyonların gelişmiş siber tehditleri önleyebilmesi amacıyla siber tehdit bilgilerine duyulan ihtiyaçların belirlenebilmesi ve bünyelerindeki doldurması gereken eksikliklerin giderilebilmesi amacıyla Zack Bilgi Boşluğu analizi gerçekleştirilmiştir.

Bu yöntem çerçevesinde, organizasyonların siber tehdit bilgilerinin paylaşımı konusunda bünyelerindeki stratejik boşluklar belirlenmiş ve bu boşlukların doldurulmasına yönelik yapılması gereken çalışmalar belirtilmiştir. Organizasyonların gelişmiş siber tehditleri önleyebilmesi amacıyla gerçekleştirmesi gereken çalışmaların belirlenebilmesi için Maslow'un İhtiyaçlar Hiyerarşisinden faydalanılmıştır.

5.1. Analiz 1 - Zack Bilgi Boşluğu Analizi

Çalışmanın 2. bölümünde M. Zack tarafından öne sürülen Zack Bilgi Boşluğu yöntemine değinilmiştir. Bu bölümde ise organizasyonların tehditlerle mücadelede bünyelerinde hangi

bilginin geliştirilmesi veya edinilmesi gerektiğini belirleyebilmesi için Zack Bilgi Boşluğu analizinden faydalanılmıştır.

Bu analizde, bilgi temelli kaynaklarının ve yeteneklerinin stratejik bir değerlendirmesini yapmış olan bir organizasyonun hangi bilginin geliştirilmesi veya edinilmesi gerektiğini belirleyebileceği öne sürülmektedir. Bir organizasyon bünyesindeki bilgi boşluğunu ve stratejik boşluğu belirlediğinde, hangi bilginin geliştirilmesi veya elde edilmesi gerektiğine karar verebilmektedir.

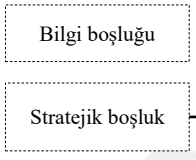
Bu kapsamda, organizasyonlarda tehdit bilgilerine duyulan ihtiyaçların belirlenebilmesi ve eksikliklerin giderilebilmesi amacıyla Zack Bilgi Boşluğu yönteminden faydalanılmıştır. Bu bağlamda, temel seviyede siber tehdit bilgisine sahip olan bir organizasyon olduğu varsayılarak organizasyonun sahip olduğu bilgiler, bilmesi gerekilenler, bilinenlerle neler yapılabileceği ve neler yapılması gerektiği hususları incelenmiştir.

Organizasyonların bilinen ve geleneksel siber tehditleri önleyebilmesi için en azından temel seviyede siber tehdit bilgisine sahip olması gerektiği değerlendirilmektedir. Sahip olunan bu bilgiler ile tehditlere yönelik mücadele edebilecektir. Organizasyonların gelişmiş siber tehditleri bertaraf edebilmesi için ise siber tehditler, siber tehdit aktörleri, saldırı grupları ve saldırganların özelliklerine (Saldırganların taktikler, teknikler ve prosedürleri vb.) ilişkin daha fazla bilgiye sahip olması gerekmektedir. Organizasyonların mevcut tehdit bilgisi kapasitesini geliştirmesi ve daha fazla bilgi elde edebilmesi için yayımlanan siber güvenlik zafiyetleri, güvenlik uyarıları, güvenlik yamaları ve tehdit raporlarını takip etmesi gerekmektedir.

Çizelge 5.1.'de organizasyonların Zack Bilgi Boşluğu analizi kapsamında dikkate alması gereken hususlar belirtilmiştir.

Çizelge 5.1. Organizasyonlar için Zack Bilgi Boşluğu analizi

Organizasyon ne biliyor?	Organizasyonunuz ne bilmelidir?
▪ Temel düzeyde siber tehdit bilgisi (İndikatörler, kötücül yazılım türlerinin karakteristiği, kara listedeki IP adresleri ve alan adları, güvenlik uyarıları, tehdit bilgisi raporları ve araç konfigürasyonları bileşenleri vb.)	▪ Zenginleştirilmiş siber tehdit bilgisi (Siber tehditler, siber tehdit aktörleri, saldırı gruplarının ve saldırganların özelliklerine dair bilgiler, saldırganların taktikler, teknikler ve prosedürleri vb.) ▪ Yayımlanan siber güvenlik zafiyetleri, güvenlik uyarıları, güvenlik yamaları ve tehdit raporları takip edilmeli ve bu bilgiler elde edilmeli
Organizasyonunuz bildikleriyle neler yapabilir?	Organizasyonunuz bildikleriyle ne yapmalıdır?
▪ Geleneksel siber tehditler tespit edilebilir ▪ Bu bilgiler ışığında tehditler bertaraf edilebilir ▪ Veri kaynakları çeşitlendirilebilir, farklı veri kaynakları incelenebilir ▪ Farklı veri kaynaklarından elde edilen veriler analiz edilebilerek mevcut bilgiler zenginleştirilebilir ▪ Mevcut bilgileri paylaşarak diğer paydaşların kapasitelerinin artması sağlanabilir ▪ Elde edilen bilgilerden yararlanılarak hangi bilgi varlıklarının ve sistemlerinin risk altında olduğu belirlenebilir ▪ Durumsal farkındalık artırılabilir ▪ Elde edilen bilgiler ışığında gelişen tehdit örüntüleri belirlenebilir ▪ Zararlı girişimler izlenebilir ▪ Saldırganların teknik, taktik ve prosedürleri anlaşılabilir ▪ Tehdit oluşturabilecek noktalara doğru çözüm önerileri sunulabilir, önlemler daha bilinçli yapılandırılabilir ▪ Gelecekteki gelişmiş tehditler için tehdit analizinde ileri görüş kazanılabilir	▪ İşbirliği ekosistemine katılım sağlanmalı ▪ Sahip olunan tehdit bilgileri paylaşılmalı ▪ İşbirliği çalışmaları genişletilmeli ▪ Diğer paydaşların bilgi ve birikiminde faydalanılmalı ▪ Elde edilen bilgiler ile yeni savunma stratejileri geliştirilmeli ▪ Saldırılara karşı kullanılan önlemler geliştirilmeli ▪ Gelişmiş saldırılara yönelik gerçek zamanlı önlemler alınmalı ▪ Saldırıların kaynağına yönelik aksiyon alınmalı ▪ Proaktif bir yaklaşım benimsenmeli, potansiyel tehditler araştırılmalı ▪ Muhtemel saldırılar hakkında taktik ve teknik yöntemler keşfedilmeli ▪ İş süreçleri ve güvenlik politikalarını destekleyen bilgi paylaşım hedefleri belirlenmeli Savunma teknolojilerine, güvenlik ekiplerine ve savunma programlarına ilişkin yatırımlar planlanmalı ▪ Bütçe yapılandırmaları yapılmalı



Gerçekleştirilen analiz neticesinde, organizasyonların mevcut siber tehdit bilgisi kapasitesini zenginleştirerek bünyelerindeki bilgi boşluğunu, bilgi paylaşımı yaparak ve tehditler hakkında diğer paydaşlarla birlikte mücadele ederek stratejik boşluğu doldurabileceği değerlendirilmektedir.

Organizasyonlar;

- Bünyelerindeki mevcut bilgiler ile veri kaynaklarını çeşitlendirilerek ve farklı veri kaynaklarını inceleyerek mevcut siber tehdit bilgisi kapasitesini zenginleştirilebilir.
- Sahip oldukları bu bilgileri zenginleştirerek Zack Bilgi Boşluğu analizinde yer alan bilgi boşluğunu giderebilir.
- Siber tehditler ve siber tehdit aktörleri hakkında daha fazla bilgiye sahip olabilir.
- Hangi bilgi varlıklarının ve sistemlerinin risk altında olduğunu belirleyebilir, tehdit oluşturabilecek noktalara doğru çözüm önerileri sunabilir.

Organizasyonların Zack Bilgi Boşluğu analizindeki stratejik boşluğu giderebilmesi için ise;

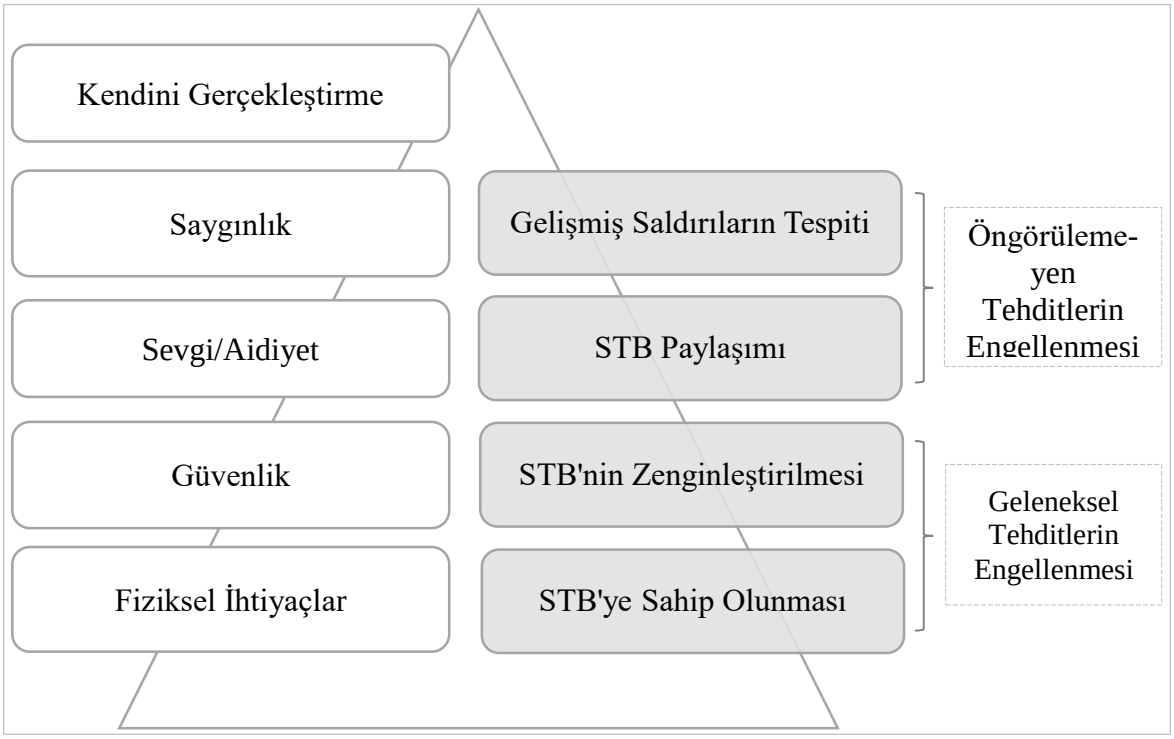
- Siber tehditler hakkında daha fazla bilgiye erişilmelidir.
- Diğer paydaşlarla işbirliği yapılmalı, paydaşların bilgi ve deneyimlerinden faydalanılmalı, sahip olunan tehdit bilgilerini paydaşlarla paylaşarak işbirliğine katkı sağlanmalı, işbirliği çalışmaları genişletilmelidir.
- Elde edilen bilgiler ile gelişmiş siber tehditlerin önlenebilmesi için yeni savunma stratejileri geliştirilmeli, saldırılara karşı kullanılan önlemler geliştirilmeli, gelişmiş saldırılara yönelik gerçek zamanlı önlemler alınmalı, saldırıların kaynağına yönelik aksiyon alınmalı, proaktif bir yaklaşım benimsenmeli, potansiyel tehditler araştırılmalı, muhtemel saldırılar hakkında taktik ve teknik yöntemler keşfedilmelidir.
- İş süreçleri ve güvenlik politikalarını destekleyen bilgi paylaşım hedefleri belirlenmeli, savunma teknolojilerine, güvenlik ekiplerine ve savunma programlarına ilişkin yatırımlar planlanmalı ve bütçe yapılandırmaları yapılmalıdır.

Bu sayede, organizasyondaki ilave öneri, doğrulama ve düzeltmeler paylaşılarak göstergelerin iyileştirilebilmesi sağlanabilecek, gelişen tehdit örüntüleri belirlenebilecek ve tehdit oluşturabilecek noktalara doğru çözüm önerileri sunulabilecektir.

5.2. Analiz 2 – Maslow'un İhtiyaçlar Hiyerarşisi Analizi

Organizasyonların siber tehdit bilgilerinin paylaşıldığı bir ekosisteme dâhil olması ile birlikte, mevcut bilgisinin artması ve olgunlaşması, diğer paydaşların bilgisinden faydalanarak güvenlik seviyelerinin artması, tehditleri algılama yeteneklerinin gelişmesi ve koruyucu önlemler için güvenlik stratejilerinin geliştirilmesi mümkün olabilecektir. Bu çerçevede, organizasyonlar siber tehdit bilgisinin önemini kavramalı, siber tehdit bilgisinin organizasyonlara sağlayacağı faydalara odaklanmalı ve bir paylaşım modeline katılması halinde elde edebileceği avantajların farkına varması gerekmektedir.

Bu kapsamda, organizasyonlar tarafından siber tehdit bilgisi kapasitesinin geliştirilmesi amacıyla yerine getirilmesi gerekilen faaliyetlerin analizinin gerçekleştirilebilmesi amacıyla Maslow'un İhtiyaçlar Hiyerarşisinden faydalanılmıştır. Maslow'un İhtiyaçlar Hiyerarşisinde kullanmış olduğu metodoloji, organizasyonların siber tehdit bilgisine olan ihtiyaçları, gelişmiş siber tehditlerin engellenmesi amacıyla yapması gereken faaliyetler ve organizasyonlara sağlayacağı avantajlar bağlamında incelendiğinde Şekil 5.1.'de yer alan aşamalar oluşmaktadır.



Şekil 5.1. Organizasyonlar için Maslow'un İhtiyaçlar Hiyerarşisi analizi

Organizasyonlar için siber uzayda ortaya çıkan tehditlerin engellenmesi öncelikli faaliyetlerden birisidir. Bu bağlamda organizasyonlar, öncelikli olarak geleneksel ve bilinen siber tehditleri tespit ederek, bu tehditlerin ortadan kaldırılmasına odaklanmalıdır. Sonraki aşamada ise bilinmeyen ve öngörülemeyen gelişmiş siber tehditleri tespit etmeye çaba göstermelidir.

Gerçekleştirilen Maslow'un İhtiyaçlar Hiyerarşisi analizinde, Maslow İhtiyaçlar Hiyerarşisine benzer şekilde organizasyonlarda siber güvenlik bağlamındaki temel gereksinimlerin karşılanmasının ardından güvenlik çalışmalarını artıracak çalışmalara ağırlık verilmesi gerekmektedir. Siber tehdit bilgisine sahip olunması siber tehditlerle mücadelede temel oluşturmakta olup, organizasyonların bu tehditlerle mücadele edebilmesi amacıyla öncelikle temel düzeyde siber tehdit bilgisine sahip olması gerekmektedir. Bu sayede, siber tehditlere karşı gerekli tedbirlerin alınabilmesi, tehdit raporları veya tehdit bilgisi platformları aracılığıyla yayımlanan tehdit verileri doğrultusunda bilinen siber tehditlerin engellenebilmesi mümkün olabilecektir.

İkinci aşamada ise tehditlerle mücadelenin etkin bir şekilde yürütülebilmesi amacıyla mevcut yeteneklerin artırılması ve siber güvenlik kapasitesinin geliştirilmesi gerekmektedir. Bu çerçevede, sahip olunan veya elde edilen siber tehdit bilgilerinin zenginleştirilmesi ve farklı kaynaklardan gelen verilerin analiz edilmesi ile eyleme geçirilebilir siber tehdit bilgisinin elde edilmesi gerekmektedir. Organizasyonların siber tehdit bilgisi veri kaynaklarını çeşitlendirmesi, farklı tehdit bilgisi raporlarını incelemesi, güvenlik uyarılarını takip etmesi, bu konuda gerekli bütçe ve envanter yatırımlarını gerçekleştirmesi ve personel kaynağı sağlaması gerekmektedir. Bu sayede, siber güvenlik kapasitesi artırılarak ve siber tehdit bilgisi yetenekleri zenginleştirilerek öngörülemeyen diğer tehditlerin tespit edilmesi mümkün olabilecektir.

Üçüncü aşamada ise Maslow Hiyerarşisine benzer şekilde bir önceki basamaktaki minimum gereksinimleri sağladıktan sonra siber dünyadaki diğer paydaşlarla etkileşime geçilmeli ve işbirliği çalışmaları gerçekleştirilmelidir. Gerçek dünyada sosyal çevreler oluşturulduğu gibi siber dünyada da organizasyonların etkileşimde bulunma, diğer paydaşların bilgi birikiminden faydalanma ihtiyaçları bulunmaktadır. Ayrıca siber güvenliğin temel unsurlarından biri de diğer paydaşlarla işbirliği yapılması olup,

organizasyonların siber dünyada etkileşimde bulunması ve paydaşlarla tecrübe paylaşımı yapması gerekmektedir.

Paydaşlarla siber tehditlere yönelik bilgi, deneyim ve tecrübe paylaşımı yapılması tüm paydaşların siber güvenlik kapasitesinin artmasına katkı sağlayacaktır. Bu aşamada, organizasyonlar tarafından bilgi paylaşım çalışmalarına katılım sağlanması ve diğer paydaşların teşvik edilmesi, siber tehditlere ilişkin bilgilerin zamanında paydaşlarla paylaşmasına katkı sağlayacaktır. Bu kapsamda, paydaşlar arasında veri, bilgi, deneyim paylaşımına imkân tanıyacak altyapının oluşturulması, siber tehdit bilgisine sahip olan organizasyonlar arasında bilgi paylaşılmasına olanak tanıyacak bir işbirliği platformunun oluşturulması faydalı olacaktır. Bu sayede her bir paydaşın siber güvenlik kapasitesinin artması ve siber tehditlerle topyekûn mücadele edilmesi mümkün olabilecektir.

Dördüncü aşamada ise; organizasyonların gelişmiş siber saldırıları ve/veya tehditleri tespit etmesine odaklanması gerekmektedir. Organizasyonlar bilgi paylaşımı platformu sayesinde diğer paydaşlardan da elde ettiği bilgiler doğrultusunda kapasitelerini daha da artırabilecek ve siber tehditlere ilişkin daha fazla bilgi sahibi olabilecektir.

Bu sayede, geleneksel siber saldırıların yanı sıra APT ve yapay zekâ temelli, daha gelişmiş saldırıların engellenmesi mümkün olabilecektir. Zira siber aktörler her geçen dün daha da dinamik bir yapıya bürünmekte ve sürekli olarak taktik, teknik ve prosedürlerini değiştirebilmektedir. Bu kapsamda, organizasyonlar, elde ettikleri siber tehdit bilgisi ile gelişmiş tehditleri bertaraf edebilecektir. Ayrıca bu sayede, reaktif savunmadan proaktif korumaya geçilmesi sağlanabilecek ve bilinmeyen siber tehditlere yönelik organizasyonlar tarafından gerekli önlemlerin alınmasına yardımcı olunabilecektir.

Sonuç olarak, organizasyonların siber tehditlerin önlenmesine yönelik kurumsal stratejilerini ve politikalarını daha efektif bir şekilde belirleyebilmesi, siber güvenlik problemlerini tespit etmesi ve bu problemlere yönelik çözüm oluşturabilmesi ve siber saldırıların kaynağına yönelik aksiyon alabilmesi mümkün olabilecektir.

5.3. Zack Bilgi Boşluğu ve Maslow'un İhtiyaçlar Hiyerarşisi Analizlerinin Birlikte Değerlendirilmesi

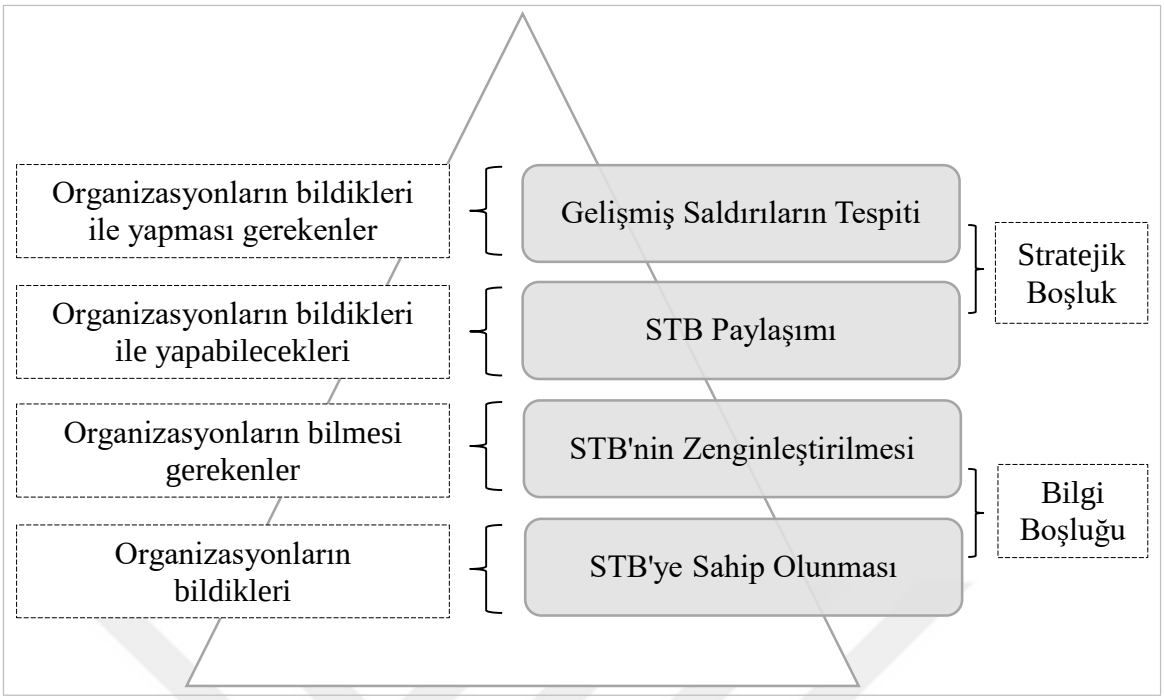
Çalışmanın bu bölümünde, organizasyonların Maslow'un İhtiyaçlar Hiyerarşisi analizinde belirtilen çalışmaları gerçekleştirdikçe Zack Bilgi Boşluğu analizinde belirlenen bilgi boşluğunu ve stratejik boşluğu doldurup dolduramadığının belirlenebilmesi amacıyla Maslow'un İhtiyaçlar Hiyerarşisi ve Zack Bilgi Boşluğu analizleri birlikte değerlendirilmiştir.

Zack Bilgi Boşluğu analizi kapsamında, organizasyonların gelişmiş siber tehditleri engelleyebilmesi için zenginleştirilmiş siber tehdit bilgisine sahip olması, diğer paydaşlarla işbirliği yaparak kapasitesini geliştirmesi ve bünyelerinde bulunan bilgi boşluğunu ve stratejik boşluğu gidermesi gerektiği değerlendirilmiştir.

Maslow'un İhtiyaçlar Hiyerarşisi analizi kapsamında ise organizasyonların siber tehditlerle etkin bir şekilde mücadele edebilmesi ve gelişmiş saldırıları önlemeye odaklanması amacıyla siber tehditler ve tehdit aktörleri hakkında daha fazla bilgi sahibi olabilmesi ve bu bilgileri zenginleştirmesi için diğer paydaşlarla işbirliği yaparak kapasitesini geliştirmesi gerektiği değerlendirilmiştir.

Organizasyonlar için ele alınan Zack Bilgi Boşluğu analizi ile Maslow İhtiyaçlar Hiyerarşisi birlikte değerlendirildiğinde ise Maslow Hiyerarşisinin ilk iki basamağında yer verilen organizasyonların sahip oldukları siber tehdit bilgisini farklı veri kaynaklarını analiz ederek zenginleştirmesi ve geleneksel ve bilinen siber tehditleri engelleyebilecek kapasiteye ulaşması ile Zack Bilgi Boşluğu analizinde belirlenen bilgi boşluğunu doldurabileceği değerlendirilmektedir.

Maslow'un İhtiyaçlar Hiyerarşisinin 3. ve 4. basamaklarında belirtilen ve işbirliği yapılarak gelişmiş siber tehditlerin tespit edilmesine yönelik kapasiteye sahip olunması ile Zack Bilgi Boşluğu analizinde belirlenen stratejik boşluğun doldurabileceği değerlendirilmektedir. Şekil 5.2.'de Maslow'un İhtiyaçlar Hiyerarşisindeki basamaklarda yer alan çalışmaları gerçekleştirdikçe Zack Bilgi Boşluğu analizinde belirlenen boşlukların giderilebileceği belirtilmektedir.



Şekil 5.2. Zack Bilgi Boşluğu ve Maslow Hiyerarşisinin birlikte değerlendirilmesi

Sonuç olarak, Maslow Hiyerarşisi analizinde belirtildiği üzere, organizasyonların sahip oldukları bilgileri zenginleştirerek bünyelerindeki bilgi boşluğunu, diğer paydaşlarla işbirliği yapmak suretiyle kapasitelerini artırarak bünyelerindeki stratejik boşluğu doldurabileceği değerlendirilmektedir. Organizasyonlar, bünyelerindeki bilgi boşluğunu ve stratejik boşluğu doldurarak sahip olunan siber tehdit bilgisi ile siber güvenlik çalışmaları kapsamında ihtiyaç duyulan bilgi kapasitesini artırabilecektir.

Örnek olarak bir üniversitenin siber güvenlik çalışmaları incelendiğinde, Zack Bilgi Boşluğu analizi ile üniversite bünyesindeki siber tehditlerin tespiti ve bilgi paylaşımı konusundaki bilgi boşluğu ve stratejik boşluk belirlenebilmektedir. Zack Bilgi Boşluğu analizi gerçekleştirilerek bilgi boşluğu ve stratejik boşluk belirlendiğinde, hangi bilginin geliştirilmesi veya elde edilmesi gerektiğine karar verilebilmektedir.

Ayrıca Maslow Hiyerarşisi analizi kullanılarak üniversitenin gelişmiş siber tehditleri tespit etme ve engellemeye yönelik gerekli kapasiteye sahip olması için gerçekleştirmesi gereken çalışmalar belirlenebilmektedir. Üniversitenin, sahip olduğu bilgileri farklı kaynaklardan elde ettiği bilgiler doğrultusunda zenginleştirmesi ile geleneksel ve bilinen siber tehditleri engelleyebilecek kapasiteye ulaşabilecektir. Bu sayede bünyesindeki bilgi boşluğunu giderebilecektir.

Bunun yanında, gelişmiş siber tehditlerin tespit edilmesi ve engellenmesi amacıyla üniversite bünyesindeki tehdit bilgilerinin zenginleştirilmesi ve siber tehditler hakkında daha fazla bilgi edinilmesi amacıyla diğer paydaşlarla işbirliği çalışmaları gerçekleştirilmelidir. Böylelikle, siber tehditler ve siber tehdit aktörleri hakkında daha fazla bilgiye sahip olunabilecek ve muhtemel saldırılar hakkında bilgi sahibi olunabilecektir. Böylelikle, organizasyonların bünyelerindeki stratejik boşluğu doldurabileceği ve gelişmiş saldırıları engelleyebilecek yeteneğe sahip olabileceği değerlendirilmektedir.

Sonuç olarak, üniversite tarafından Maslow Hiyerarşisinde yer alan çalışmaların yerine getirilmesi siber tehdit bilgisi kapasitesini artıracak, diğer paydaşlarla işbirliği yaparak sahip olduğu bilgileri zenginleştirebilecektir. Bu sayede, üniversite bünyesinde bulunan ve Zack Bilgi Boşluğu analizinde belirlenen bilgi boşluğu ve stratejik boşluk giderilebilecek, siber tehditlere karşı daha hazırlıklı olunabilecektir.

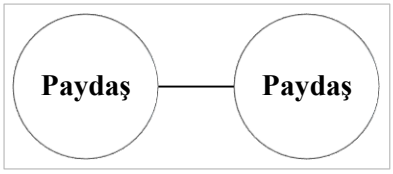
5.4. Siber Tehdit Bilgisi Paylaşım Modeli Önerisi

Ülkemizde siber tehditlere, siber olaylara ve güvenlik zafiyetlerine ilişkin bilgi paylaşımı USOM vasıtasıyla gerçekleştirilmektedir. Bunun yanı sıra, ülkemizde USOM tarafından gerçekleştirilen çalışmaların yanı sıra Savunma Sanayi Başkanlığı, BTK, TÜBİTAK gibi kurumlar ile birlikte Siber Güvenlik Kümelenmesi gibi organizasyonlar tarafından siber güvenlik ekosisteminin geliştirilmesi amacıyla çalışmalar yürütülmektedir.

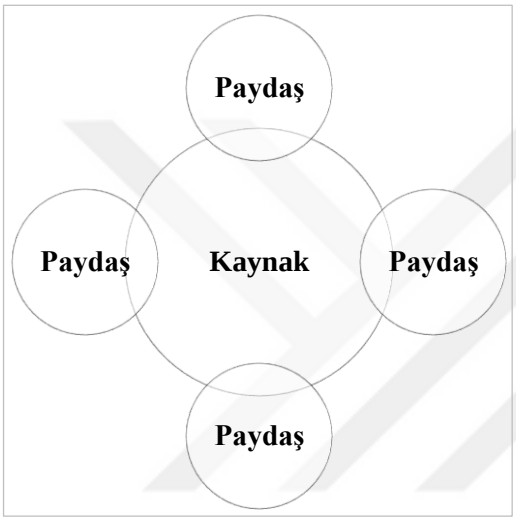
USOM tarafından, siber tehditleri önlemek amacıyla alarm, uyarı ve duyuru faaliyetleri yürütülmektedir. USOM tarafından siber tehditlere yönelik gerçekleştirilen bilgilendirme faaliyetlerine, kamu kurumları ve kritik altyapı sektörlerinde faaliyet gösteren kuruluşlar dâhil olmaktadır. Ayrıca söz konusu yapıda USOM'dan SOME'lere ve SOME'lerden USOM'a olmak üzere çift yönlü paylaşım yapılmaktadır.

Diğer taraftan, literatürde tehdit bilgisi paylaşımında kullanılan modeller incelendiğinde genellikle 3 paylaşım modelinin yaygın olarak kullanıldığı belirlenmiştir. Tehdit bilgisi paylaşımı, paydaşlar arasında genellikle "Peer-to-peer, Eşler Arası", "Peer-to-hub, Kaynak – Paydaş (Merkezi kaynaktan diğer paydaşlara bilgi akışı)" ve "Hibrid" olmak üzere 3

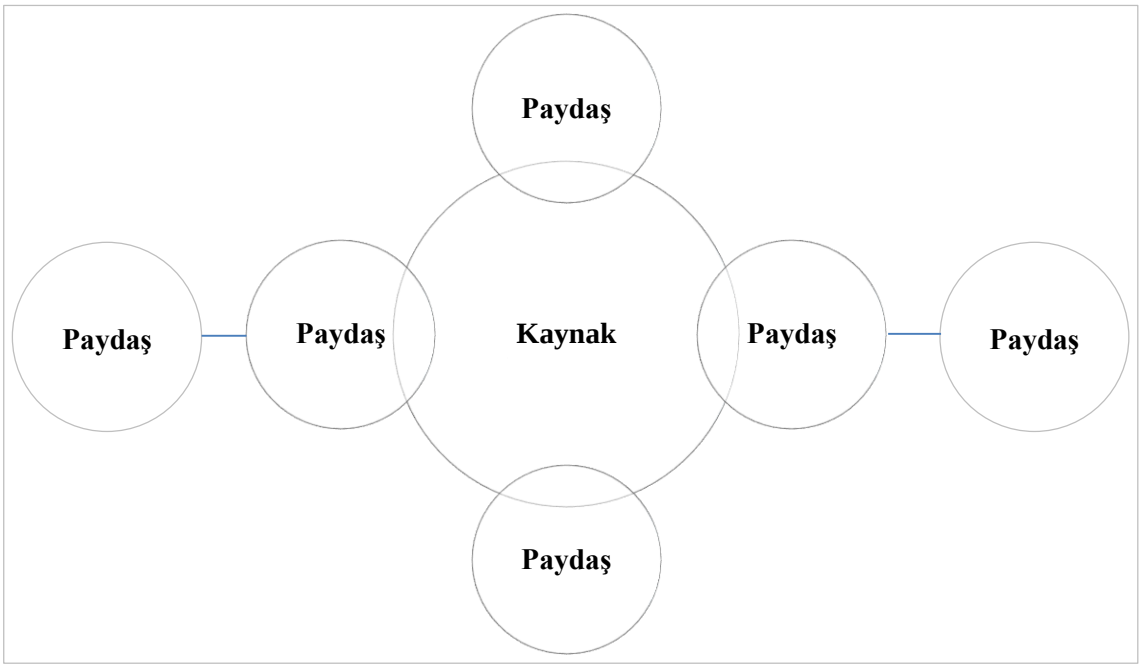
şekilde gerçekleştirilmektedir [1]. Söz konusu paylaşım modelleri, Şekil 5.3., Şekil 5.4. ve Şekil 5.5.'te belirtilmiştir.



Şekil 5.3. Paydaştan paydaşa paylaşım modeli [1]



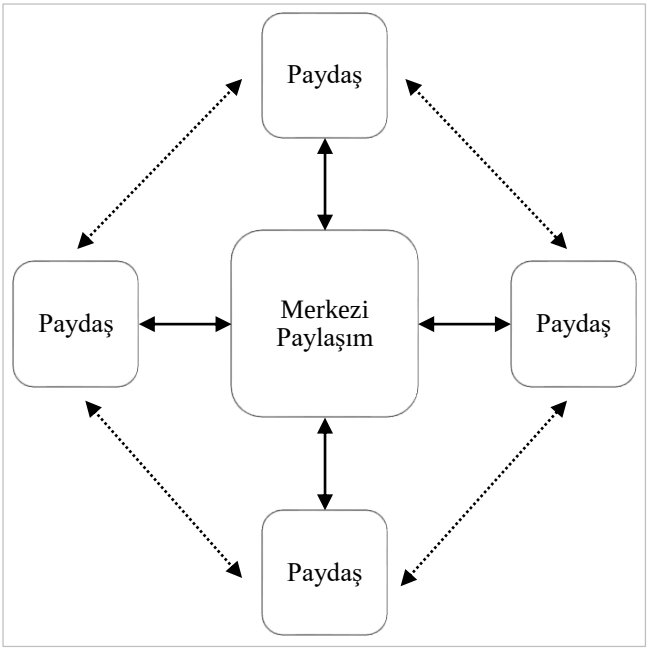
Şekil 5.4. Kaynaktan paydaşa paylaşım modeli [1]



Şekil 5.5. Hibrid paylaşım modeli [1]

Bunun yanında, Ming Liu ve arkadaşları tarafından yapılan çalışmada ise siber tehdit bilgisi paylaşım sürecinin üç modelle tanımlanabildiği ifade edilmekte, belirtilen modellerin; "Peer to peer, Eşler Arası", "Source-subscriber, Kaynak – Paydaş (Kaynaktan diğer paydaşlara bilgi akışı)" ve "Hub-and-spoke, Merkez – Paydaş (Paydaşlardan sağlanan tehdit bilgilerinin tüm paydaşlarla paylaşılması)" olduğu vurgulanmaktadır. Ayrıca "hub and spoke" modelinin, gelecek nesil tehdit bilgisi paylaşım sistemlerinin geliştirilmesi için geniş çapta kabul gördüğü belirtilmektedir [8]. "Peer to peer - Eşler Arası" modelinde, paydaşlar tehdit bilgilerini bazı standartlara ve anlaşmalara göre birbirleriyle paylaşmakta, "Source-subscriber" modelinde paydaşlar tek bir üreticiden paylaşılan tehdit bilgisini almakta, "Hub-and-spoke" modelinde ise merkezi bir birimin, birden çok işbirlikçiden sağlanan tehdit bilgilerini aldığı ve analiz ettiği, akabinde işlenen tehdit bilgilerinin paydaşlarla paylaşıldığı ifade edilmektedir.

Türkiye'deki USOM ve SOME'ler vasıtasıyla yürütülen paylaşım modeli "Source-subscriber" paylaşım modeli ile benzerlik göstermektedir. Ülkemizde organizasyonlar arasında oluşturulması önerilen paylaşım modelinin ise Wagner ve arkadaşları tarafından belirtilen "hibrid paylaşım" modeline benzer şekilde oluşturulmasının daha etkin bir bilgi paylaşım imkânı sunacağı düşünülmektedir. Şekil 5.6.'da hibrid paylaşım modeline benzer şekilde oluşturulması önerilen paylaşım modeli belirtilmiştir.



Şekil 5.6. Önerilen paylaşım modeli

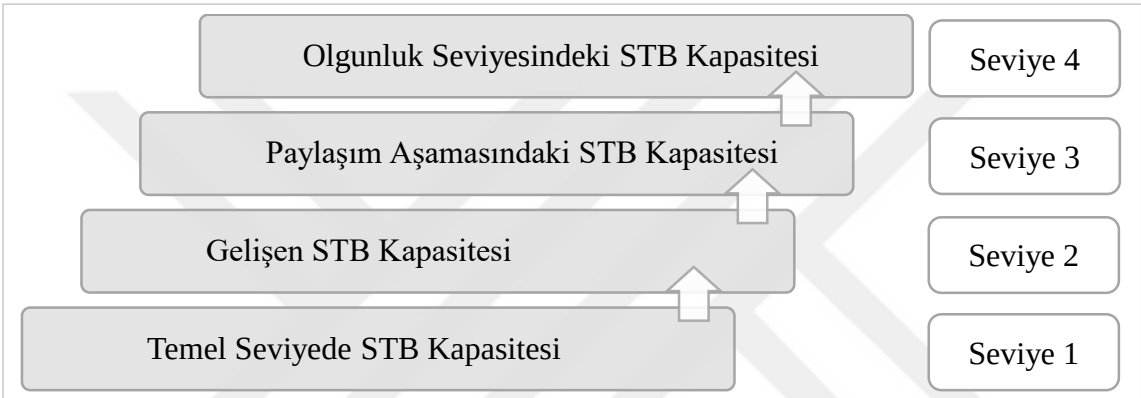
Türkiye'de oluşturulması önerilen paylaşım modelinde, her paydaşın merkezi paylaşım kaynağı ve diğer paydaşlarla çift yönlü bilgi alışverişi yapabilmesi önerilmektedir. Bu paylaşım modelinde, diğer paylaşım modellerinden farklı olarak diğer paydaşlarla doğrudan bağlantılar kurulabilmesi, tehditlere yönelik hızlı aksiyon alınabilmesi, organizasyonların diğer paydaşların bilgi, deneyimleri ve çalışmaları hakkında bilgi edinebilmesi hedeflenmiştir. Ayrıca özellikle aynı veya benzer sektördeki paydaşlar arasında işbirliği ve bilgi paylaşımının artırılması, belirli sektörleri hedef alan tehditlerin daha kolay engellenebilmesi ve tehdit bilgisi kapasitesinin geliştirilmesi amaçlanmıştır.

Ayrıca önerilen paylaşım platformunda, hangi bilginin hangi paydaşla paylaşılacağının kontrol edilmesi ve platformda anonim bilgi paylaşımına imkân veren bir işlevsellik sağlanmasının faydalı olacağı düşünülmektedir. Önerilen modelde bir organizasyonla ilgili bir güvenlik zafiyetinin tespit edilmesi halinde, güvenlik risklerinin en aza indirilmesi amacıyla bu bilgilerin her paydaşla paylaşılması yerine yalnızca ilgili paydaş ile paylaşılmasına olanak sağlanabilmektedir. Böylece bir organizasyon tarafından sadece bir organizasyonu ilgilendiren bir zafiyet tespit edildiğinde, herhangi bir güvenlik riski oluşturmayacak şekilde sadece ilgili organizasyonla bu bilgiler paylaşılabilecektir.

Bununla birlikte, önerilen paylaşım platformunda tehditlerin hızlı bir şekilde algılanabilmesi ve paylaşılabilmesi amacıyla paydaşlar arasında ortak bir dilin kullanılması önerilmektedir. Ayrıca paylaşılan bilgilerin paydaşlarla bu ortak dil üzerinden standart bir formda paylaşılması ve içeriğinde belirli seviyedeki bilgileri barındırması gerektiği değerlendirilmektedir. İlave olarak, her paydaşın paylaşılan tehditlere yönelik gerekli önlemleri hızlı bir şekilde alabilmesi, zaman kayıplarının önlenebilmesi ve müşterek çalışmaların önüne geçilebilmesi için platformda paydaşlarla paylaşılan tehdit bilgilerinin yanında bu tehditlere yönelik çözüm önerilerinin de paylaşılmasının faydalı olacağı düşünülmektedir.

Öte yandan, önerilen modele hangi organizasyonların katılım sağlayacağının belirlenebilmesi ve organizasyonların tehdit bilgisi düzeyinin belirlenebilmesi amacıyla bir olgunluk modeli önerilmektedir. Bu modele göre, tehdit bilgilerinin paylaşılmasına yönelik paylaşım yeteneklerini tamamlayan organizasyonların platforma dâhil edilmesi gerektiği değerlendirilmektedir.

Bu kapsamda, organizasyonların işbirliği platformuna dâhil olabilmesi için bir olgunluk modeli geliştirilmiştir. Bu olgunluk modelinin, organizasyonlar tarafından siber tehdit bilgisi paylaşım çabalarının olgunluk düzeyinin değerlendirilmesi ve sistematik ve aşamalı bir şekilde daha yüksek olgunluk düzeylerine geçilmesi için bir çerçeve olarak kullanılabileceği değerlendirilmektedir. Bir organizasyonun siber tehdit bilgisi paylaşım kapasitesi ve çabası genişledikçe daha yüksek bir olgunluk düzeyine doğru ilerlenecek ve organizasyonun elde edeceği kazanımlar artacaktır. Şekil 5.7.'de önerilen olgunluk modeli ve seviyeleri belirtilmiştir.



Şekil 5.7. Olgunluk modeli

Olgunluk modelinin birinci seviyesi sistematik olmayan bir şekilde, yayımlanan tehdit raporları üzerinden siber tehdit bilgisinin edinildiği başlangıç aşamasını ifade etmektedir. Bu seviyede organizasyonlar, herhangi bir işbirliği platformuna katkıda bulunmadan sahip olunan mevcut bilgileri kullanmaktadır. Organizasyonların bu seviyede gelişmiş siber tehditleri tespit edebilecek kapasiteden yoksun olduğu ve tehdit raporları üzerinden elde ettiği bilgiler doğrultusunda bilinen siber tehditleri tespit edebilecek kapasiteye sahip olduğu varsayılmaktadır.

İkinci seviyede ise organizasyonlar, sahip oldukları siber tehdit bilgilerini farklı kaynaklardan gelen bilgiler ile zenginleştirmektedir. Bu seviyeye ulaşan organizasyonlar, siber tehdit bilgilerini geleneksel bilgi kaynaklarından manuel olarak toplamakta ve bu bilgileri analiz etmektedir. Organizasyonlar bu aşamada siber tehdit bilgisi raporlarını inceleyerek ve güvenlik uyarılarını takip ederek siber tehdit bilgisi veri kaynaklarını çeşitlendirmektedir. Bu seviyede, mevcut siber tehdit bilgisinin zenginleştirilerek

öngörülemeyen diğer tehditlerin tespit edilmesine imkân veren kapasiteye sahip olunabilmektedir.

Üçüncü seviyeye ulaşan organizasyonlar ise diğer paydaşlarla paylaşıma aktif olarak katılacak kapasiteye sahip olmakta ve belirledikleri tehdit bilgilerini paylaşmaktadır. Bu seviyede diğer paydaşlarla etkileşime geçilmekte ve işbirliği yapılmaktadır. Bu seviyede organizasyonlar, diğer paydaşlarla paylaşım gerçekleştirebilecek düzeyde tehdit bilgilerine sahip olmakta ve siber güvenlik kapasitesini geliştirmektedir.

Dördüncü seviyedeki organizasyonlar ise paylaşım modeli aracılığıyla elde ettikleri bilgiler ile gelişmiş siber saldırıları ve/veya tehditleri engelleyebilecek kapasiteye sahiptir. Organizasyonlar bilgi paylaşımı platformu sayesinde siber kapasitelerini daha da artırmakta ve daha etkin siber tehdit bilgisine sahip olmaktadır. Bu sayede, geleneksel siber saldırıların yanı sıra APT ve yapay zekâ temelli daha gelişmiş saldırıların engellenmesine yönelik kapasiteye sahip olunmaktadır.

Sonuç itibarıyla, önerilen işbirliği modelinin bir platforma dönüştürülmesi ve paydaşların anlamlı bir katkı sağlayabilmesi amacıyla yeterli düzeyde siber tehdit bilgisi üretebilmesi ve bunları paydaşlarla paylaşabilmesi gerektiği değerlendirilmiştir. Organizasyonların tehdit bilgisi kapasitelerini geliştirerek olgunluk seviyelerini artırması ve platforma katkı sunabilecek seviyeye gelmesi gerekmektedir. Bu kapsamda, önerilen işbirliği platformuna dâhil olunabilmesi için organizasyonların en az 3. seviyede olgunluk seviyesine sahip olması gerektiği, henüz 3. seviyeye ulaşmayan organizasyonların ise 3. seviyeye geldikten sonra platforma dâhil edilmesinin gerektiği değerlendirilmiştir.

6. SONUÇ

Siber tehditlerle mücadele edilebilmesi için; gelişen siber tehditlere yönelik gerekli tedbirlerin gerçek zamanlı ve hızla alınması, bilgi paylaşımı ve işbirliğinin sağlanması, deneyim ve en iyi uygulamaların paylaşılması ve paylaşılan verilerin değerlendirilmesi önem arz etmektedir. Bu tez çalışması kapsamında, siber tehdit bilgisi paylaşımı ile ilgili olarak dünyadaki önemli ülke çalışmaları incelenmiş, ülkemizde tehdit bilgisi paylaşımı konusunda gerçekleştirilen çalışmalara yönelik analizler gerçekleştirilmiş, model önerileri yapılmış, elde edilen bulgular paylaşılmış ve önerilerde bulunulmuştur.

Bu çalışma kapsamında;

- Siber tehdit bilgilerinin paylaşılmasına yönelik en yaygın kullanılan ülke modelleri incelenmiş, ülkemizde tehdit bilgisi paylaşımı konusunda gerçekleştirilen çalışmalar Maslow'un İhtiyaçlar Hiyerarşisi ve Zack Bilgi Boşluğu analizinden faydalanılarak değerlendirilmiş, mevcut durum analizleri gerçekleştirilmiş ve öneriler sunulmuştur.
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Rehberi ilk kez Maslow'un İhtiyaçlar Hiyerarşisi ve Zack Bilgi Boşluğu metodu ile analiz edilmiştir.
- Organizasyonların gelişmiş siber tehditleri önleyebilmesi için tehdit bilgilerine duyulan ihtiyaçların belirlenebilmesi ve gerçekleştirilmesi gerekilen çalışmaların belirlenebilmesi için Zack Bilgi Boşluğu analizi ve Maslow'un İhtiyaçlar Hiyerarşisi analizinden faydalanılmış ve model önerilerinde bulunulmuştur.
- Ülkemizde organizasyonlar arasında bilgi paylaşım platformunun oluşturulması önerilmiş ve önerilen paylaşım platformunu daha anlaşılır hale getirmek için örnekler sunulmuştur.
- Siber Tehdit İttifakı ile AB ülkelerindeki bilgi paylaşım çalışmaları incelenmiş, bu paylaşım platformunun katkıları somutlaştırılmış ve bu katkıların ulusal siber güvenlik ekosistemine faydaları gözden geçirilmiştir.
- İlgili organizasyonların istifade edebileceği değerlendirmeler yapılmış ve öneriler sunulmuştur.

Tez kapsamında yapılan incelemelerdeki tespitlerimiz aşağıda sunulmuştur:

- ABD ve AB'de siber tehditlere ilişkin organizasyonlar arası bilgi paylaşımının gerçekleştirildiği işbirliği modelleri bulunmaktadır.
- Ülkemizde organizasyonlar açısından bakıldığında, siber güvenlik şirketleri arasında tehdit bilgisinin paylaşıldığı bir işbirliği mekanizması bulunmamaktadır.
- Ülkemizde, USOM tarafından siber tehditlerin önlenmesi amacıyla alarm, uyarı ve duyuru faaliyetleri yürütülmekte, tehdit bilgisi paylaşımı ise kamu kuruluşlarındaki ve sektörde oluşturulan SOME'ler ile kullanılan bir platform üzerinden gerçekleştirilmektedir.
- Ulusal Siber Güvenlik Stratejileri ve Eylem Planları kapsamında (yayımlanan eylem planları incelendiğinde), bu konunun açık olarak değerlendirildiği bir çalışmaya rastlanmamıştır.

Tez kapsamında yapılan incelemelerdeki değerlendirmelerimiz ve önerilerimiz aşağıda sunulmuştur:

- Siber Vatanda yüksek seviyeli koruma sağlanabilmesi ve savunma direncinin artırılması için işbirliğinin gerekli olduğu ve bu çalışmaların geliştirilmesi gerektiği değerlendirilmiştir.
- Organizasyonların birbirleriyle etkileşime girebileceği ve bilgi ve deneyim paylaşabileceği bir platform oluşturulmasının faydalı olacağı, işbirliklerini artıracağı ve sağlanan işbirliği ile gelişmiş veya öngörülemeyen siber tehditlerin tespit edilebileceği değerlendirilmiştir.
- Ülkemizde Siber Tehdit İttifakına (CTA) benzer şekilde siber güvenlik organizasyonları arasında bilgi paylaşımının gerçekleştirildiği işbirliği platformu oluşturulmalıdır.
- Siber tehdit bilgisi paylaşımı konusunda önerilen hususların, organizasyonların hem verileri değerlendirme hem de tehditlerle ortaklaşa mücadele etmelerine katkı sağlayacak önemli bir boşluğu doldurabileceği değerlendirilmektedir.
- İşbirliği platformu ile organizasyonların bilgi paylaşım çalışmaları genişletilerek siber olayların analizi ve kötü amaçlı yazılım analizleri hakkında bilgi toplanması, depolanması, dağıtılması ve paylaşılmasının mümkün olabileceği öngörülmektedir.

- Önerilen paylaşım platformu ile;
  - Organizasyonların siber güvenliğine önemli ölçüde katkı sağlanacağı,
  - Mevcut ürünlerin iyileştirilebileceği veya yeni ürün geliştirmenin önünü açacağı,
  - Paydaşlar arasında müşterek Ar-Ge çalışmaları gerçekleştirilerek yerli ve milli siber güvenlik ürünlerin geliştirilebileceği,
  - Yapay zekâ ve makine öğrenmesi gibi teknolojiler kullanılarak yeni analiz yöntemlerinin geliştirilebileceği

  öngörülmektedir.
- Ülkemizde tehdit bilgisi paylaşımında faaliyetleri bulunan ilgili kümelenmelerin, organizasyonların veya kurumların bu çalışmadan faydalanabileceği ve çalışmanın bu kuruluşlara katkı sağlayabileceği düşünülmekte olup, Siber Güvenlik Kümelenmesi gibi oluşumlara tehdit bilgisi paylaşımı konusunda fikir verebileceği değerlendirilmektedir.
- Önerilen paylaşım platformu bir ülke modeli olmayıp, siber güvenlik firmaları arasında işbirliğinin sağlanması amacıyla oluşturulan Siber Güvenlik Kümelenmesinde uygulanabileceği değerlendirilmektedir.
- Siber Güvenlik Kümelenmesinde hâlihazırda paydaşlar arasında doğrudan bilgi paylaşımının hedeflenmediği değerlendirilmekte olup, Kümelenme bünyesinde tehdit bilgisi paylaşım çalışmalarının geliştirilmesinin faydalı olacağı değerlendirilmektedir.
- İşbirliği mekanizmasına katılan her paydaşın siber güvenlik kapasitesinin ve yetkinliğinin artacağı gerçeğinden hareketle işbirliği konusunda farkındalığın arttırılması ve organizasyonların işbirliğine teşvik edilmesi yerinde olacaktır.

Bu tez çalışması kapsamında, organizasyonlar için önerilen paylaşım modelinde, her paydaşın merkezi paylaşım kaynağı ve diğer paydaşlarla çift yönlü bilgi alışverişi yapabilmesi önerilmekte olup, çalışmada ayrıca;

- Diğer paylaşım modellerinden farklı olarak diğer paydaşlarla doğrudan bağlantılar kurulabilmesi, tehditlere yönelik hızlı aksiyon alınabilmesi, organizasyonların diğer paydaşların bilgi, deneyimleri ve çalışmaları hakkında bilgi edinebilmesi hedeflenmiştir.

- Aynı veya benzer sektördeki paydaşlar arasında özellikle işbirliği ve bilgi paylaşımının artırılması, belirli sektörleri hedef alan tehditlerin daha kolay engellenebilmesi ve tehdit bilgisi kapasitesinin geliştirilmesi amaçlanmıştır.
- Paylaşım platformunda;
  - Hangi bilginin hangi paydaşla paylaşılacağının kontrol edilmesi, bir paydaşa özgü güvenlik risklerinin sadece ilgili paydaşla paylaşılması ve platformda anonim bilgi paylaşımına imkân veren bir işlevsellik sağlanmasının bilgi paylaşımının efektif bir şekilde gerçekleştirilmesine katkı sağlayacağı değerlendirilmiştir.
  - Tehditlerin hızlı bir şekilde algılanabilmesi ve paylaşılabilmesi için paydaşlar arasında ortak bir dilin kullanılması, ayrıca zaman kayıplarının ve müşterek çalışmaların önüne geçilebilmesi için paylaşılan tehdit bilgilerinin yanında çözüm önerilerinin de paylaşılmasının faydalı olacağı değerlendirilmiştir.
  - Hangi organizasyonların bulunacağı veya katılım sağlayacağının belirlenebilmesi ve paydaşların tehdit bilgisi kapasitelerinin ölçülebilmesi amacıyla bir olgunluk modeli önerilmiştir.
  - Olgunluk modelinin, tehdit bilgisi paylaşım çabalarının olgunluk düzeyinin değerlendirilmesi ve sistematik ve aşamalı bir şekilde daha yüksek düzeylere geçilmesi için bir çerçeve olarak kullanılabileceği değerlendirilmiştir. Bir organizasyonun siber tehdit bilgisi paylaşım kapasitesi ve çabası genişledikçe daha yüksek bir olgunluk düzeyine doğru ilerlemesi ve organizasyonun elde edeceği kazanımların bu sayede artırılması hedeflenmiştir.

Diğer taraftan, bu çalışmanın Türkiye'deki siber güvenlik çalışmalarına katkı sağlayabilmesi, tehdit bilgisi paylaşımı konusundaki çalışmaların hayata geçirilebilmesi amacıyla gelecek araştırmacılar için önemli bir kaynak olabileceği düşünülmekte olup, gelecek araştırmacılar için öneriler ile dikkat edilmesi gereken hususlar aşağıda sunulmuştur:

- Çalışmanın konuyla ilgili araştırmacılar, kurum/kuruluşlar veya organizasyonlar tarafından değerlendirilebileceği, önerilen platformun denenmesi için açık bir platform oluşturulabileceği ve diğer araştırmacılarla paylaşılabileceği değerlendirilmektedir.
- Bu çalışma tehdit bilgisi paylaşımında kullanılan en yaygın modeller referans alınarak hazırlanmış olup, gelecekteki araştırmacılar tarafından çalışmanın kapsamının

genişletilerek dünya genelinde kullanılan diğer modellerin ve çalışmaların da incelenip iyileştirilebileceği değerlendirilmektedir.

- Çalışmada incelenen Siber Tehdit İttifakının ABD'deki siber güvenlik firmaları arasında oluşturulmuş bir bilgi paylaşım platformu olması sebebiyle konuya dair yasal düzenlemeler çalışma kapsamına alınmamıştır. Bu sebeple, gelecekteki çalışmacılar tarafından konuyla ilişkili yasal düzenlemelerin de çalışma kapsamına alınabileceği değerlendirilmektedir.
- Siber Vatan terminolojisi analiz edilerek tehdit bilgisi paylaşımına bakış açısının genişletilebileceği değerlendirilmektedir.
- Türkiye'de siber güvenlik alanında hazırlanacak olan gelecek çalışmalarda, bu tez çalışmasında sunulan sonuçların dikkate alınabileceği, özellikle 2020-2023 Ulusal Siber Güvelik Stratejisi ve Eylem Planının alt eylem maddelerinin oluşturulması aşamasında bu çalışmada analiz edilen ve önerilen hususların değerlendirilebileceği düşünülmektedir.
- Ayrıca önerilen modelin kapsamlı olması ve tehdit bilgisi paylaşımının çok yönlü olması sebebiyle oluşabilecek güvenlik risklerini de dikkate alarak kapsamlı bir bilgi paylaşım platformu oluşturulması faydalı olacaktır.
- Ülkemizde USOM'un bu konuya en fazla katkı sağlayan merkez olduğu ve USOM yapısı içerisinde Kurumsal ve Sektörel SOME'ler olduğu bilinmektedir. Bu yapılanma içerisinde, farklı SOME yapıları için bu tez kapsamında önerilen modelin kullanılması faydalı olacaktır.
- Siber tehdit istihbaratı veya bilgisi toplama, siber tehditlere yönelik alınacak önlemler açısından çok önemlidir. Siber tehdit bilgilerinin toplanması, değerlendirilmesi ve paylaşılması için yapay zekâ ve makine öğrenmesi gibi yeni teknolojilerin geliştirilmesi ve kullanılmasının faydalı olacağı düşünülmektedir.
- Ülkemizde Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının yayımlanmadan önce Hizmet Kalitesi-Boşluk Modeli, Karar Verme Modeli ve Bilgi Boşluğu Karar Teorisi gibi farklı analiz araçlarıyla test edilmesi, oluşabilecek stratejik, taktiksel veya operasyonel bilgi boşluklarının veya stratejik boşlukların önceden tespit edilerek giderilmesine katkı sağlayabilecektir.

KAYNAKLAR

1. Wagner, T. D., Mahbub, K., Palomar, E., and Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87, 1-13.

2. Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, 30(1), 53-65.

3. Mkuzangwe, N. N., and Khan, Z. C. (2020). Cyber-threat information-sharing standards: a review of evaluation literature. *The African Journal of Information and Communication*, 25, 1-12.

4. Conti, M., Dargahi, T., and Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. *In Cyber Threat Intelligence*,1-6.

5. Abu, M. S., Selamat, S. R., Ariffin, A., and Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.

6. Murdoch, S., and Leaver, N. (2015). Anonymity vs. trust in cyber-security collaboration. *In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, Colorado USA, 27-29.

7. Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S., and Reid, E. (2012). Conceptual framework for cyber defense information sharing within trust relationships. *IEEE In 2012 4th International Conference on Cyber Conflict (CYCON 2012*), Tallinn, Estonia, 1-17.

8. Liu, M., Xue, Z., He, X., and Chen, J. (2019). Cyberthreat-intelligence information sharing: Enhancing collaborative security. *IEEE Consumer Electronics Magazine*, 8(3), 17-22.

9. Kokkonen, T., Hautamäki, J., Siltanen, J., and Hämäläinen, T. (2016). Model for sharing the information of cyber security situation awareness between organizations. *IEEE In 2016 23rd International Conference on Telecommunications (ICT)*, Thessaloniki, Greece, 1-5.

10. Win, K. M. N., and Thaw, Y. M. K. K. (2019). Information Sharing of Cyber Threat Intelligence with their Issue and Challenges. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 3(5), 878-880.

11. Mutemwa, M., Mtsweni, J., and Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. *IEEE In 2017 Conference on Information Communication Technology and Society (ICTAS)*, Durban, South Africa, 1-6.

12. Zibak, A., and Simpson, A. (2018). Can We Evaluate the Impact of Cyber Security Information Sharing? *IEEE In 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Glasgow, Scotland, 1-2.

13. Aydın A. (2019). *Devlet Egemenliğinin Dönüşümünde Dijital Verinin Araçsal İlişkisi ve Rolü*. Doktora Tezi, Hacı Bayram Veli Üniversitesi Bilişim Enstitüsü, Ankara.

14. Hill, R. (2015). Dealing with cyber security threats: International cooperation, ITU, and WCIT. *IEEE In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia, 119-134.

15. İnternet: Definition of Cybersecurity. International Telecommunication Union. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, Son Erişim Tarihi: 10.01.2021.

16. Yılmaz, S., ve Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 323-331.

17. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., and Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, 89, 349-359.

18. İnternet: Muscat, I. (2019). Cyber Threats, Vulnerabilities and Risks. Acunetix. URL: https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/, Son Erişim Tarihi: 16.12.2020.

19. İnternet: Robinson, N., Gribbon, L., Horvath V. and Robertson, K. (2013) Cybersecurity Threat Characterisation. Rand Cooperation. URL: https://www.rand.org/pubs/research_reports/RR235.html, Son Erişim Tarihi: 10.01.2021.

20. İnternet: Ross, R. S. (2019). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf, Son Erişim Tarihi: 10.01.2021.

21. Mavroeidis, V. and Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *IEEE In 2017 European Intelligence and Security Informatics Conference (EISIC)*, Athens, Greece, 91-98.

22. İnternet: Understanding Cyber Threat Intelligence Operations - CBEST Intelligence-Led Testing. (2016). Bank of England. URL: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf, Son Erişim Tarihi: 10.01.2021.

23. İnternet: Cyber Threat Intelligence In Government: A Guide For Decision Makers & Analysts. (2019). UK Digital, Data & Technology. URL: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf, Son Erişim Tarihi: 10.01.2021.

24. Wagner, T. D. (2019). Cyber Threat Intelligence for "Things". *IEEE In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Oxford, UK, 1-2.

25. İnternet: Threat Intelligence Definition. Why Threat Intelligence is Important for Your Business and How to Evaluate a Threat Intelligence Program. Kaspersky. URL: https://www.kaspersky.com/resource-center/definitions/threat-intelligence, Son Erişim Tarihi: 10.01.2021.

26. İnternet: Gourley B. (2018) Security Intelligence at the Strategic, Operational and Tactical Levels. URL: https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/-6.

27. İnternet: Actionable Information for Security Incident Response. (2014). European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/publications/actionable-information-for-security, Son Erişim Tarihi: 10.01.2021.

28. Feledi, D., Fenz, S., and Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, 17(4), 199-209.

29. Brown, S., Gommers, J., and Serrano, O. (2015). From cyber security information sharing to threat management. *In Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, Colorado, USA, 43-49.

30. Garrido-Pelaz, R., González-Manzano, L., and Pastrana, S. (2016). Shall we collaborate? A model to analyse the benefits of information sharing. *In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, Vienna, Austria, 15-24.

31. İnternet: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). (2012). MITRE Corporation. URL: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the, Son Erişim Tarihi: 10.01.2021.

32. İnternet: Impe, K. V. (2015). How STIX, TAXII and CybOX Can Help With Standardizing Threat Information. Security Intelligence. URL: https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information, Son Erişim Tarihi: 16.12.2020.

33. İnternet: Connolly, J., Davidson, M. and Schmidt, C. (2014). The Trusted Automated eXchange of Indicator Information (TAXII™). URL: https://taxiiproject.github.io/getting-started/whitepaper, Son Erişim Tarihi: 16.12.2020.

34. İnternet: Threat Intelligence Platform. Wikipedia. URL: https://en.wikipedia.org/wiki/Threat_Intelligence_Platform, Son Erişim Tarihi: 10.01.2021.

35. İnternet: Clean, P. P. (2015). Automated Defense - Using Threat Intelligence to Augment. URL: https://www.sans.org/reading-room/whitepapers/threats/paper/35692, Son Erişim Tarihi: 10.01.2021.

36. İnternet: Features of MISP, The Open Source Threat Sharing Platform. Malware Information Sharing Platform Project. URL: https://www.misp-project.org/features.html, Son Erişim Tarihi: 16.12.2020.

37. İnternet: IBM X-Force Threat Intelligence. International Business Machines (IBM). URL: https://www.ibm.com/security/xforce, Son Erişim Tarihi: 16.12.2020.

38. İnternet: Moriarty, K. M. (2013). Transforming Expectations For Threat-Intelligence Sharing. RSA Security Inc. URL: http://docplayer.net/13281555-Transforming-expectations-for-threat-intelligence-sharing.html, Son Erişim Tarihi: 10.01.2021.

39. Dandurand, L., and Serrano, O. S. (2013). Towards improved cyber security information sharing. *IEEE In 2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, Estonia, 1-16.

40. İnternet: Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way Sponsored by Infoblox. (2018). Ponemon Institute. URL: https://www.infoblox.com/wp-content/uploads/infoblox-white-paper-ponemon-infoblox-2018-final-report.pdf, Son Erişim Tarihi: 10.01.2021.

41. İnternet: Northcutt, S. (2015). Who's Using Cyberthreat Intelligence and How? SANS Institute. URL: https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf, Son Erişim Tarihi: 10.01.2021.

42. İnternet: Goodwin, C. and Nicholas, J. P. (2015). A framework for cybersecurity information sharing and risk reduction. Microsoft. URL: https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf, Son Erişim Tarihi: 10.01.2021.

43. İnternet: Zheng D. E. and Lewis, J. A. (2015). Cyber Threat Information Sharing. Center for Strategic and International Studies (CSIS). URL: http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf, Son Erişim Tarihi: 15.03.2021.

44. Bauer, J. M., and Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy,* 33(10-11), 706-719.

45. İnternet: Threat Intelligence. (2018). Sothis Tech. URL: https://www.sothis.tech/en/threat-intelligence-i/, Son Erişim Tarihi: 10.01.2021.

46. Abouzahra, M., and Tan, J. (2014). The effect of community type on knowledge sharing incentives in online communities: A meta-analysis. *IEEE In 2014 47th Hawaii International Conference on System*, Waikoloa, USA, 1765-1773.

47. Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H., and Gholipour, R. (2013). Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, 68, 223-232.

48. Haustein, M., Sighart, H., Titze, D., and Schoo, P. (2013). Collaboratively Exchanging Warning Messages between Peers While under Attack. *IEEE In 2013 International Conference on Availability, Reliability and Security*, Regensburg, Germany, 726-731.

49. Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence, *Cryptography and Security*, 1-12.

50. İnternet: Glossary of Key Information Security Terms. (2019). National Institute of Standards and Technology (NIST). URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, Son Erişim Tarihi: 10.01.2021.

51. İnternet: Warsaw Summit Key Decisions. (2017) North Atlantic Treaty Organization (NATO). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf, Son Erişim Tarihi: 10.01.2021.

52. İnternet: Warsaw Summit Communiqué. (2016). North Atlantic Treaty Organization (NATO). URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, Son Erişim Tarihi: 15.01.2021.

53. Polat, D. Ş. (2020). NATO'nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi, (International Security Congress Special Issue),* 135-158.

54. Desmet P. and Fokkinga S. (2020). Beyond Maslow's Pyramid: Introducing a Typology of Thirteen Fundamental Needs for Human-Centered Design. *Multimodal Technologies and Interaction*, 4(3), 1-22.

55. İnternet: Ulusal Siber Güvenlik Stratejisi ve 2020 – 2023 Eylem Planı. (2021). Ulaştırma ve Altyapı Bakanlığı. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf, Son Erişim Tarihi: 10.01.2021.

56. Zack, M. (1999). Developing a Knowledge Strategy. *California Management Review*, 125-145.

57. İnternet: Johannes D. Knowledge Management: Developing a Knowledge Strategy, Businessoft Consulting. URL: http://www.businessoft-indonesia.com/Pdf/Developing_a_Knowledge_Strategy.pdf, Son Erişim Tarihi: 10.01.2021.

58. İnternet: FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing. (2015). White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/02/12/fact-sheet-

executive-order-promoting-private-sector-cybersecurity-inform, Son Erişim Tarihi: 10.01.2021.

59. İnternet: Information Sharing and Analysis Organizations (ISAOS). Cybersecurity & Infrastructure Security Agency. URL: https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos, Son Erişim Tarihi: 11.01.2021.

60. İnternet: Kenway, J. (2020). Getting to Know CTA: Part 1 — A Community of Practice. Cyber Threat Alliance. URL: https://cyberthreatalliance.org/getting-to-know-cta-part-1, Son Erişim Tarihi: 16.12.2021.

61. İnternet: Cyber Threat Alliance. (2014). URL: https://www.cyberthreatalliance.org, Son Erişim Tarihi: 16.12.2021.

62. İnternet: The Cyber Kill Chain. Lockheed Martin. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, Son Erişim Tarihi: 16.12.2020.

63. İnternet: Daniel, M. (2020). Looking Back On 2020. Cyber Threat Alliance. URL: https://www.cyberthreatalliance.org/looking-back-on-2020, Son Erişim Tarihi: 15.01.2021.

64. İnternet: Jarvis, J. (2020). Fighting Malware Means Strength in Numbers. Cyber Threat Alliance. URL: https://www.cyberthreatalliance.org/fighting-malware-means-strength-in-numbers, Son Erişim Tarihi: 15.01.2021.

65. İnternet: Information Sharing and Analysis Centres (ISACs) Cooperative Models. (2018). European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, Son Erişim Tarihi: 15.01.2021.

66. İnternet: Public Private Partnerships (PPP) Cooperative Models. (2018). European Union Agency for Cybersecurity (ENISA) URL: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models, Son Erişim Tarihi: 10.01.2021.

67. İnternet: Cyber Security Information Sharing Partnership (CISP). National Cyber Security Centre. URL: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp, Son Erişim Tarihi: 16.12.2020.

68. İnternet: What is the Cybersecurity Information Sharing Partnership (CISP)? UK-CERT. URL: https://www.octf.gov.uk/OCTF/media/OCTF/images/publications/Cybercrime/CiSP-leaflet.pdf?ext=.pdf, Son Erişim Tarihi: 10.01.2021.

69. İnternet: Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. (2012). Resmi Gazete. URL: https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm, Son Erişim Tarihi: 10.01.2021.

70. İnternet: Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. (2013). Ulaştırma ve Altyapı Bakanlığı. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf, Son Erişim Tarihi: 10.01.2021.

71. İnternet: Bilgi ve İletişim Güvenliği Rehberi. (2020). Dijital Dönüşüm Ofisi Başkanlığı. URL: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, Son Erişim Tarihi: 10.01.2021.

72. İnternet: Sektörel SOME Kurulum ve Yönetim Rehberi. (2014). Ulaştırma ve Altyapı Bakanlığı. URL: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/sektorel-some-reh.pdf, Son Erişim Tarihi: 10.01.2021.

73. İnternet: Siber Güvenliğimizi Artırma Azim Ve Kararlılığı İçerisindeyiz. (2018). Bilgi Teknolojileri ve İletişim Kurumu. URL: https://www.btk.gov.tr/haberler/siber-guvenligimizi-artirma-azim-ve-kararliligi-icerisindeyiz, Son Erişim Tarihi: 10.01.2021.

74. Işık, Z. E. (2019). *Siber Güvenlik Ekosisteminin Geliştirilmesi*. Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara, 180-182.

75. İnternet: Türkiye Siber Güvenlik Kümelenmesi. (2017). URL: https://www.siberkume.org.tr/Index, Son Erişim Tarihi: 11.01.2021.

76. İnternet: Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi. (2019). Resmi Gazete. URL: https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf, Son Erişim Tarihi: 10.01.2021.

GAZİ GELECEKTİR..