Düzce Üniversitesi
Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Açık Kaynak İstihbaratı Üzerinden Siber Saldırı Tespiti Yöntemleri

Ali EKŞİM [a,b*], Mustafa KARA [b,c]

[a] *TÜBİTAK BİLGEM UEKAE, PK 74, 41470 Gebze, Kocaeli, TÜRKİYE*
[b] *MSÜ, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, TÜRKİYE*
[c] *Mustafa Kemal Üniversitesi, Hatay, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: ali.eksim@tubitak.gov.tr*

ÖZET

Son yıllarda siber suçun gittikçe büyüyen etkisi, siber tehditlerin üstesinden gelmek için dünya çapında istihbarat ve kanun uygulayıcı kurumlar ortaya çıkartmıştır. Tüm kurum ve kuruluşlar siber suçla en iyi şekilde nasıl mücadele edileceğini öğrenmeye çalışmaktadır. İnternet ağ teknolojilerinin gelişmesi ve genişlemesi ile siber saldırıları engellemek gittikçe zorlaşmaktadır. Ağdaki tehlikeli hedeflerin kapsamlı bir analizini oluşturmak için internette açık halde bulunan verileri toplayarak istihbarat elde etmek, istihbarat birimleri için önemli bir araç olarak hızla gelişmektedir. İnternetteki mevcut açık kaynakların miktarı hızla arttıkça, siber suçla mücadele gelişen açık kaynak istihbaratı yani OSINT yöntemleri çerçevesinde daha etkin olmaktadır. Buna bağlı olarak bilginin etkili ve verimli bir şekilde toplanması ve işlenmesi için gelişmiş yazılım araçları ve teknikleri daha da gelişmektedir. Bu çalışmada, OSINT kavramı siber saldırı tespiti için her açıdan ele alınmıştır. OSINT kavramını internet ortamında kamuya açık paylaşılan veriler üzerinden tarama, bulma, toplama, çıkarma, kullanma, doğrulama ve analiz yaparak elde etme amaçlı destek yöntemleri detaylandırılarak anlatılmıştır. Siber tehditlere karşı geliştiren araştırmalar için açık kaynak verilerinin kullanılmasına yönelik mevcut çabalar gözden geçirilmiş ve detaylı bir şekilde incelenmiştir. Bunlara ek olarak, siber suçlarla etkin mücadele için siber suç soruşturma çerçevesi önerilmiştir.

Anahtar Kelimeler: *Açık Kaynak İstihbaratı, Güvenlik, OSINT, Saldırı Tespiti, Siber Savunma*

Cyber Attack Detection Methods over Open Source Intelligence

ABSTRACT

In recent years, the growing impact of cybercrime has revealed worldwide intelligence and law enforcement agencies to overcome cyber threats. All institutions and organizations are trying to learn how to fight cybercrime in the best possible way. With the development and expansion of internet networking technologies, it becomes increasingly difficult to prevent cyber attacks. It is rapidly developing as an important tool for intelligence units by collecting data on the internet to generate a comprehensive analysis of dangerous targets on the network. As the amount of available open-source resources on the internet increases rapidly, the emerging open-source intelligence, in other words, is more effective within the framework of OSINT methods. In this connection,

Geliş:10/12/2018, Düzeltme:13/01/2019, Kabul: 17/01/2019

advanced software tools and techniques are further developed for the effective and efficient collection and processing of information. In this study, the concept of OSINT was discussed in all aspects for cyber attack detection. The purpose of browsing, finding, collecting, extracting, using, verifying and analyzing the OSINT concept through publicly available data is explained in detail. Existing efforts to use open source data for research against cyber threats have been reviewed and examined in detail. In addition, the cyber crime investigation framework has been proposed to combat cybercrime effectively.

Keywords: *Open Source Intelligence, Security, OSINT, Attack Detection, Cyber Defense*

I. GİRİŞ

Türkiye'de ve dünyada son yüzyıl içinde, dijital dünya eksenindeki siber saldırılar nerden ele alınırsa alınsın hızlı ve tehlikeli bir girişim içinde hareket etmektedir. Halka açık erişilebilir kaynakların kullanımı yoluyla, dijital dünya, modern topluma muazzam avantajlar sağlamış, fakat aynı zamanda bilgi güvensizliği sorunlarına, ağın kırılganlık haritasındaki noktalarda artmalara yani ağlardaki güvenlik açıklarının artışına ve bilişim sistemlerinde zayıflıklara yol açmıştır [1]. İnternetin herkese açık ve paylaşımlı altyapısı, tüm kullanıcılar arasında iç içe geçmiş güvenlik açıkları yaratma potansiyeli oluşturmaktadır [2]. Bu açıkları örneklemek gerekirse virüsler, bilgisayar korsanları, güvenli ve özel bilgilerin sızması, sistem hataları ve hizmetlerin kesintiye uğraması gibi açıklar olağandışı bir akışta ortaya çıkmaktadır. Bu ortamda tüm siber saldırı mantığına sahip suçluların suç işlemek için dört temel yönteme sahip oldukları anlaşılmaktadır. Bunlar sırasıyla:

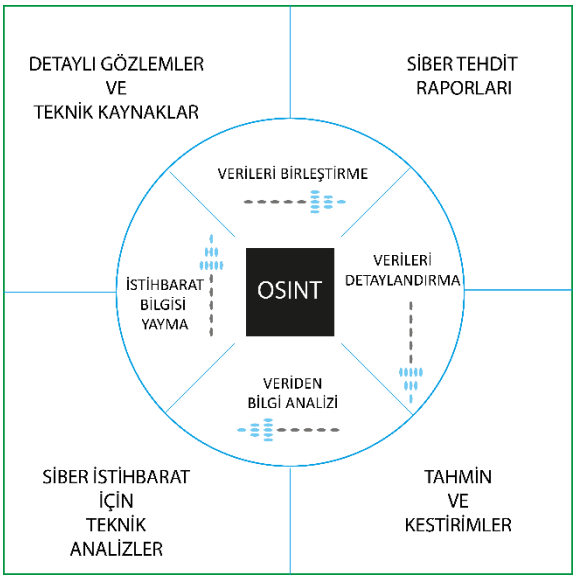
- Siber suçlulara daha iyi fırsatlar ve altyapı sunan küreselleşme süreci,
- Dağıtık sistem ile bütün sistemin tek bir ağ gibi olması ve her ağın saldırılara açık hale gelmesi,
- Uzaktan bağlantı teknolojilerinin son kullanıcıyı daha fazla mağdur etmesi,
- Siber tehditler üzerinden çevrimiçi bilgilerin ele geçirilmesi ile yeni tehditler oluşturan mobil uygulamalar.

Mobil iletişim teknolojisinin her alanda geniş kullanımı ve ilerlemesi açık kaynakların istihbarat, politika ve iş alanlarında da yaygın kullanılmasının önünü açtı. Geleneksel haber kaynakları ve bilgi kanalları (haber kaynakları, veri tabanları, ansiklopediler, vb.) yeni sanal alana kendi varlığını sürdürebilmek için adapte edilmeye zorlandılar. Pek çok yeni medya kaynağı (özellikle sosyal medya) kullanıcılar tarafından yeniden şekillendirilen veri içeriğinin daha çok yayılmasını sağladı. Burada bizim ele aldığımız Açık Kaynak İstihbaratı (Open Source Intelligence, OSINT) kavramı, kamuya açık bilgilerin çeşitli işlemlerden geçirilerek istihbarat elde edilmesidir. Bu istihbarat süzgecinden geçirilen veriler sınıflandırılmamış, açık ve gizli olmayan kaynaklardan elde edilmektedir.

OSINT, akademik yayınlar (araştırma yazıları, konferans yayınları, vb.), medya kaynakları (gazete, radyo kanalları, televizyon, vb.), web içeriği (web siteleri, sosyal medya, vb.), ticari olarak resmen yayınlanmamış rapor veya bilgiler (teknik raporlar, ön baskılar, patentler, çalışma evrakları, iş

belgeleri, yayınlanmamış çalışmalar ve bültenler) ve kamu verileri gibi çeşitli kamu kaynaklarını kapsamaktadır. OSINT kavramı açık kaynak tabanlı her türlü veriyi ilgili alanda çok çeşitli istihbarat kaynakları olarak kullanabilmektedir. OSINT yöntemleri veriler arası bağlantı kurma yeteneğine sahiptir. Bu açıdan sadece belirli sınırlar içerisindeki verileri bilgiye çevirerek kendini sınırlandırmaz. Aksine sınırları internet ağındaki her türlü veri olarak değerlendirir. Ayrıca teknoloji geliştikçe ve bilgi ağı genişledikçe OSINT daha da etkin olmaya devam edecektir. Böylece internet ortamında tamamen alakasız gibi duran çok çeşitli veriler istihbarat tekniklerince süzülerek istihbarat bilgisi olarak karşımıza çıkabilmektedir [3].

OSINT, hükümet birimleri, ordunun kullandığı milli savunma alanları ve şirket dünyası tarafından savunma, rekabeti sürdürmek ve rekabet avantajı sağlamak için uzun zamandır kullanılmaktadır [4]. Diğer konuları da ele almak gerekirse internet kullanıcılarının büyük bir kısmı iletişim ve ticaretten oyunlara, arkadaşlık sitelerinden yorumlar içeren günlük sitelerine kadar yasal çerçevede bazı etkinlikleri kullanırken OSINT bu bağlamda kritik bir rol oynar.



Şekil 1. *Açık Kaynak İstihbaratı Veri Değerlendirme*

Şekil 1'de çizilen şemada OSINT süreci baştan sona gösterilmektedir. Kamuya açık, gizli olmayan ve sınıflandırılmamış verilerin detaylı gözlemler yapılarak ve teknik kaynaklar kullanılarak siber suç soruşturma çerçevesinden geçirilmesi ve siber saldırı öncesi tehdit raporu oluşturulması gösterilmektedir. Veriler toplanarak bilgiye dönüştürülmesi ve bilgininde istihbarat değeri taşıması kararı için gerekli işlemler siber suç soruşturma çerçevesinde aranan esas adımdır. Bu açıdan OSINT sürecinin sıradaki aşaması verileri analiz ederek siber istihbaratı dağıtım yani yayma adımına geçmesidir. Yayılma adımında gerekli görülen istihbarat bilgisi ilgili kurum ve kuruluşlara dağıtılır. Bu bilgiler istihbarat kurumlarınca geri besleme mantığı ile geri bildirim ve yönlendirme yapılarak sonlandırılmaktadır.

Makalenin ikinci bölümünde OSINT üzerinden siber güvenlik, üçüncü bölümde siber tehditlerin sınıflandırılması, dördüncü bölümde siber suç tespit analizi, beşinci bölümde OSINT destek metotları, altıncı bölümde OSINT ile siber saldırı tehdit algoritması ve son bölümde de sonuçlar açıklanacaktır.

II. OSINT ÜZERİNDEN SİBER GÜVENLİK

Ulusal güvenlik, istihbarat, yasa uygulayıcıları ve güvenlik unsurları, insanların, kurumların ve faaliyetlerin daha uyumlu bir resmini çıkarmak için internetin açık kaynak kullanımını yaygınlaştırdı. Dünyada ileri gelen devletlerin önemli kurumlarının elindeki bulgular göstermektedir ki siber suçların sayısı artış gösterdikçe gerek devlet kurumlarının gerekse özel kurumların ortaya çıkan güvensizlik ortamından olumsuz etkilendikleri görülmüştür. Yine bu araştırmalar çerçevesinde siber güvenlik liderlerinin % 76'sı siber tehditler hakkında bu yıl daha fazla endişe duyduklarını belirtmişlerdir [5]. Siber kelimesi bilgisayar ve ağ sistemleri ile alakalı kavramdır. Siber uzay kavramında yapı donanımsal ve yazılımsal teknolojilerin bir araya gelmesiyle oluşmaktadır. Siber saldırılar ise hedef alınan ağın bilgi ve kritik altyapı sistemlerine yapılan planlı saldırılardır [6]. Gün geçtikçe artmakta olan siber saldırırlar ağ ortamındaki hassas verilerin artmasıyla birlikte giderek daha yıkıcı hale gelmektedir.

İstihbarat, bilgiye yapılan bir dizi eylemden kaynaklanan veridir. Uzun yıllar devlet kurumları tarafından ulusal güvenlik amacıyla kullanılmaktadır. Bu sistemde eylemler toplanır, analiz edilir, bütünleştirilir, yorumlanır ve yayılır. İstihbaratın nihai ürünü, sonuç çıkartabilen, değerli ve başka olaylarla bağlantılı bilgi vermesidir. Ayrıca güvenlik amaçlı belirli olasılıklara karşı önlem almak için avantajlar sağlar.

İstihbarat ancak bir mimari içerisinde olduğu sürece sağlanabilir. Bu yüzden istihbarat mimarisi oluşturulur. Bu mimari sistem, bir döngü çerçevesinden oluşmaktadır. Bilginin veri haline gelmesi süreci döngünün adım adım uygulanması ile gerçekleşebilir. Bu adımlar sırasıyla;

- İzlenecek yol ve süreç belirleme,
- Bir araya getirme,
- Bilgilerin ayıklanması,
- Bilgiden veri elde edilmesi ve verilerin analizi,
- Gerekli yerlere iletme.

Üretilen bilgiler sizin veya saldırganın amaçlarını destekleyen gerçekleri, bulguları ve tahminleri içerir. İki istihbarat yöntemi bulunmaktadır bunlar sırasıyla stratejik istihbarat ve operasyonel istihbarattan oluşmaktadır. Stratejik istihbarat, uzun süreli önem taşıyan iyi bilgilendirilmiş kararları desteklemek için üretilen bilgiler anlamına gelmektedir. Stratejik istihbarat, operasyonel istihbarat ile karşılaştırıldığında daha çeşitli ve farklı veri kaynakları hakkında bilgiye ihtiyaç duymaktadır. Operasyonel istihbarat ise stratejik istihbarata göre sınırlı bir yaşam döngüsü içerisinde hareket etmektedir. Bu sınırlı yaşam süresinden dolayı operasyonel istihbarat daha hızlı hareket ederek güncel olaylar ve kavramlar üzerinden istihbarat edinmeye çalışmaktadır.

Kritik görev alanlarında OSINT'in benimsenmesi hayati önem taşımaktadır. Genel istihbarat sağlanarak, ileri düzey uyarılar, yerel terörle mücadele, kritik altyapının korunması, felaket terörizmine ve acil durum hazırlıkları ile müdahaleye karşı savunma yapmak daha da kolaylaşabilmektedir. Bu sayede istihbarat, güvenlik ve kamu güvenliği kurumlarına, terör olaylarının suç kayıtları ve siber güvenlik tehditleri de dâhil olmak üzere çok sayıda kaynaktan büyük miktarlarda veri toplanmasına olanak sağlar.

OSINT kavramını bir başka bakış açısından ele aldığımızda internetin yaşamımız üzerindeki etkisi sürekli artmaktadır [7]. Çocuk istismarı, sahtecilik, radikalleşme, taciz, kimlik hırsızlığı ve özel bilgi sızıntılarından bilgi toplandığında Web sitelerinde, günlük sitelerde ve çevrimiçi topluluklarda sosyal olarak uygunsuz davranışlar tespit edilmiştir. Kimlik hırsızlığı ve yasadışı olarak kopyalanmış filmlerin, TV şovlarının, müzik, yazılım ve donanım tasarımlarının dağıtımı, internetin suçun etkisini nasıl artırdığının iyi bir örneğidir.

Küreselleşme, yayılma hızı, anonimi ve uygun mevzuatın olmaması ya da uluslararası anlaşmaların bulunmaması bazı suçları çok yaygınlaştırmakta ve davalar ile sonuç elde etmek bile oldukça zorlaşmaktadır. İstihbarat analistlerine göre, internet tarayıcıların, arama motorlarının, web sitelerinin, veri tabanlarının, indeksleme, arama ve analitik uygulamaların yetenekleri sayesinde çok önemli veriler elde edilebilir [8]. Bu sebepten dolayı OSINT projeleri geliştirilerek, internet üzerindeki büyük açık kaynaklardan veri toplanarak ve OSINT proje parametrelerinin kabiliyetleri artırılarak verilerin entegrasyonu gibi önemli konulara daha çok önem verilmelidir.

III. SİBER TEHDİTLERİN SINIFLANDIRILMASI

Tehdit, belirli durum veya olay olduğu anlarda güvenlik önlemlerinin yerine getirilmesini engelleyen potansiyel bir güvenlik bozucusu; saldırı ise, sistemin güvenlik altyapılarını etkisiz hale getirmeyi amaçlayan akıllı bir tehditten üretilen ani bir hücumdur. Yani bilgi sistemleri üzerinden; zarar vermek, sistemlerin işleyişini engellemek ya da bilgi çalmak için yapılan çalışmalara siber saldırı denilmektedir.

Siber saldırı, bir veya daha fazla internet bileşeninden kaynaklanan yasa dışı bir etkinliktir. Web siteleri, sohbet odaları veya e-posta gibi ve genellikle internet veya başka bir bilgisayar ağının suç unsuru olarak kullanıldığı saldırılar olarak tanımlanır [9]. Günümüze kadar çok farklı türde siber saldırı tanımlanmıştır. Bazı uzmanlar gerçek siber saldırıları yani bir çevrimiçi ortamın dışında var olmayacak olan dürüst olmayan ya da kötü niyetli eylemleri basitçe etkin olan suçlardan ayırmıştır. Gerçek siber saldırıları, kredi kartlarının kötüye kullanımı gibi saldırıların aksine, virüs yayma, değiştirme veya aldatma, ağı dinleme, yeniden oluşturma (virüs, solucan), Hizmet Reddi Saldırıları (Denial of Service (DoS) Attack /Distributed Denial of Service (DDoS) Attack) olarak kabul edilmektedir.

Günümüzde siber saldırıların giderek artmasından sebebiyle OSINT kavramının önemi ulusal güvenlik için öncelikli konulardan biri olarak ele alınmaktadır. Bu tür saldırılar, meşru ağ operasyonlarını bozmakta ve ağ aygıtlarına karşı kasıtlı olarak zararlı etkiler içermektedir [10]. Bunların yanında bir ağa aşırı yüklenebilmekte ve ağa sunulan hizmetleri yasal kullanıcılara karşı sabote edebilmektedir. Saldırganlar, normal ağ etkinliklerini bozmak için yazılım servislerindeki döngü deliklerini, hataları ve yanlış yapılandırmaları da kullanabilir.

Saldırganın asıl hedefi, hedefe yönelik bir saldırıya başlamadan önce farklı istihbarat toplama yöntemleriyle elde edilen verinin bilgiye dönüştürülmesini sağlamak ve geniş bir ağ ortamını kısıtlayarak keşif yapmaktır. Gizlilik, siber saldırıların anahtar kavramlarındandır [11]. Saldırgan temelli eylemler, çeşitli ortamlarda bulunan ücretsiz kablosuz ağ kullanımı benzeri ağ açıklarından yararlanmaktadır. Örneğin hizmet aksatma saldırısı yapılırken belirli protokoller üzerinden gizlenme gerçekleştirebilir. Saldırgan kendisi doğrudan ilgili hedefe saldırmak yerine ele geçirilen köle

bilgisayarlar üzerinden internet yönlendirmesi yaparak gizlilik maskesi oluşturmaktadır. Bu durumda saldırganı tespit etmek neredeyse mümkün değildir. Bu ve benzeri saldırılar ile siber suçlular kimlik avı, spam, şantaj, kimlik hırsızlığı ve uyuşturucu kaçakçılığı gibi kötü amaçlı aktivitelerde web tabanlı iletişimini gizlemek ve gizlenmek için çeşitli fırsatlardan yararlanmaktadır.

Bazı araştırmacılara göre siber saldırılar iki türe ayrılmaktadır: hedefli ve fırsatçı saldırılar. Hedefli saldırılarda, belirli hedeflere karşı belirli araçlar uygulanır ve bu da fırsatçı saldırılara göre daha tehlikeli bir durum oluşturmaktadır. Fırsatçı saldırılar ise, internet üzerinden rastgele dağıtılan solucanların ve virüslerin yayılmasını gerektirir.

Bilişim teknolojileri, suç grupları veya örgütlenmiş siber suçluların yaptığı dolandırıcılık, sahtecilik veya siber taciz üzerinden şantaj benzeri saldırılara karşı mücadele etmek kurumlar için çok önemlidir. Saldırganları engellemek için müdahale ve önleme sistemleri oluşturmak gerekmektedir. Saldırı senaryoları çerçevesinde kurumların veritabanı güvenliğini sağlamak, kritik altyapılara olan tehdit ve çeşitli siber saldırıları engellemek ve izlemek için gözlem merkezi kurulması önerilmektedir. Suç çetelerine karşı saldırıyı tespit, sınıflandırma ve savunma açısından ulusal güvenlik alanında savunma sanayisine ve çeşitli siber savunma kurumlarına teşvik sağlamak şarttır.

IV. SİBER SUÇ TESPİT ANALİZİ

A. UYGULAMA YÖNTEMLERİ

Siber saldırılar artık geçici ve nadir bir tehdit olmaktan çıkarak, giderek daha karmaşık saldırılar ile ağınıza nüfuz etmek ve en önemli varlıklarınıza erişim kazanmak için sosyal mühendislik ve teknik becerileri bir arada kullanan bir süreçtir. Saldırganların gelişen teknoloji ile sağladıkları karmaşıklık ve beceri düzeyindeki bu artış, siber saldırıları önlemek için tek bir çözümün yetmediğini göstermektedir.

OSINT için belirli yöntemler kullanan uzmanlar, web-link analizi, metrikler, tarama yöntemleri, kaynak haritalama, metin madenciliği, ontoloji oluşturma, günlük analizi ve örüntü tanıma yöntemleri dâhil birçok yöntem kullanmakta ve bunların yanında açık kaynakların düzenlenmesi için çeşitli yöntemlerden yararlanmaktadır. Algoritmaların geliştirilmesi hesaplamalı topoloji, hiper-grafikler, sosyal ağ analizi, bilgi keşfi ve veri madenciliği, yazılım tabanlı simülasyonlar, dinamik bilgi sistemleri analizi ve diğer teknikler üzerinden gerçekleşmektedir [12]. Siber suçların başlıca çeşitleri sistemi ele geçirmek (hacking), siber vandalizm, virüsler ve solucanlar, kimlik hırsızlığı, finansal suçlar, oltalama (phishing), siber taciz, DDOS ve siber terörizmdir [13].

OSINT için aktif ve pasif olmak üzere birçok veri toplama yöntemi bulunmaktadır. Bilgilerin açıkta bulunması onların doğrudan tespitini sağlamaz. Bu açıktaki bilgilerin OSINT tarafından verilere dönüştürülmesi belirli veri yöntemleri ile sağlanmaktadır. Açık kaynak verilerinin toplanması, depolanması ve sınıflandırılması için bazı araçlar kullanırız. OSINT verilerinin toplanması, sınıflandırılması ve depolanması için yöntemler sırasıyla; Veri Kodlama, Veri Toplama, Veri Kaynağı Detayı, Veri Depolama, Veri Keşfi ve Veri Görselleştirmeyi bu araçların öne çıkanları arasındadır.

Veri Kodlama: Kodlama terimi, bir dizi karakterin iletim veya depolama amaçları için özel bir formata konulması sürecini ifade eder. Bir web ortamında, ilgili veri kümeleri internet üzerinden yerel veya dünya çapında mevcut olan veri hizmetlerinden kurtarılmaktadır. Hizmete ve bilgi türüne bağlı olarak,

veriler farklı formatlarda sunulabilir. Modelleme platformları, düz metin, biçimlendirme dilleri ve ikili dosyalar dâhil olmak üzere veri formatlarının bir karışımı ile etkileşimde bulunmak için gereklidir.

Veri Toplama: Çeşitli kaynaklardan (örneğin, bir fabrikadaki, laboratuvardaki, tıbbi veya bilimsel ortamdaki sensörler ve okuyucular) otomatik veri toplanmasıdır. Veri toplama genellikle veri erişim noktaları ve http veya ftp sayfaları gibi web bağlantıları üzerinden yapılır.

Veri Kaynağı Tespiti: Verilerin kökenini ve veri tabanları arasındaki hareketini izleme ve kaydetme sürecini ifade etmek için kullanılır. Kaynak kavramının ardında, verilerin dinamik doğası vardır. Aynı veri kümesinin farklı kopyalarını oluşturmak yerine, değişikliklerin kaydını tutmak ve mevcut duruma yol açan sürecin bir kaydını saklamak önemlidir. Veri kaynağı, bu şekilde verilerin güvenilirliğini ve sonuçların tekrarlanabilirliğini garanti edebilir. Sonuçlardan elde edilen veri kalitesi, kaynağın kullanılabilirliği ve güvenilirliğini denetlemek ve doğrulamak açısından önemlidir. Verilerin onaylanmasında merkezi olan bilimsel veri tabanlarından kanıtlar toplanmalıdır.

Veri Depolama: Bu terim, elektronik verilerin internet üzerinden erişilen üçüncü taraf hizmetiyle depolanması pratiğine değinmektedir. Geleneksel yerel depolama (Ör. disk veya bilgisayar sürücüleri) ve taşınabilir depolama (Ör. flash sürücüler) için bir alternatiftir. Ayrıca "sunucu tabanlı depolama", "internet depolama alanı" veya "bulut depolama" olarak da adlandırılabilir. İlişkisel veritabanları şu anda verileri depolamak ve paylaşmak için en iyi seçimdir.

Veri Keşfi: Veri iyileştirme, veri keşfi ve geri çağırma, veri kalite güvencesi, değer ekleme, yeniden kullanım ve zaman içinde koruma amaçlanmaktadır. İçerik oluşturucular ve arşivciler tarafından seçim ve değerlendirme içerir. Örnek vermek gerekirse entelektüel erişimin geliştirilmesi; yedekli depolama; veri dönüşümleri bunlardan bazılarıdır. Keşif sırasında elde edilen veri bütünlüğü, bilimsel veri sayısallaştırması, paylaşımı ve entegrasyonu verinin kullanımı için kritik öneme sahiptir.

Veri Görselleştirme: Bu terim, verilerin bir resimsel veya grafik biçiminde sunulması anlamına gelir. Etkileşimli veri görselleştirmesi için bir adım daha ileriye gidersek çeşitli yollar bulabiliriz. Görselleştirmede bilgisayarları ve mobil cihazları araştırma araçları olarak kullanmak gerekir. Daha fazla ayrıntı için grafikler ve şekiller halinde gördüğünüz verileri nasıl birleştirildiğini ve nasıl işlediği ile etkileşimli kullandığını değerlendirme yaparak elde etmek veri görselleştirme tarafında önemlidir.

OSINT analitik araçları, analiz etmek ve veri madenciliği teknikleri için çerçeveler sağlar. Ayrıca veriyi tanımak, tanımlamak ve tepki vermek için analitik modeller sunan kalıpları oluşturur. Bu araçlar, vazgeçilmez özellikleri birleştirmeli ve tipik veri madenciliği tekniklerini destekleyen; sınıflandırma, regresyon, ilişkilendirme, benzerlik ve ilişkilendirme (korelasyon) ile yapay sinir ağlarını içeren entegre algoritmalar ve yöntemler içerir.

Bu tür analiz araçları, kimi açık kaynak kodlu bilgi işlem platformlarında çalışan, genellikle paralel sunucular, emtia sunucularında kümelenmeler, ölçeklenebilir dağıtılmış depolama ve Hadoop mimarisi ile NoSQL veri tabanları gibi teknolojiler kullanan, öngörücü ve belirleyici analitik uygulamalar sağlayan yazılım ürünleridir [14]. Bu yazılım ürünleri büyük veri üzerinden veriyi saklayan ve işleyen bir yapıya sahiptiler. Bahsedilen yazılımlar öncelikli olarak makine öğrenmesi ve yapay zekâ teknolojileridir. Ancak bu teknolojiler saldırılara karşı büyük miktarlarda veriyi analiz ederek siber saldırılara karşı kurumların ve kişilerin zayıflıklar için tasarlanıp kullanılmaktadır.

B. SİBER TEHDİTLERİN TESPİTİ VE ÖNLENMESİ

Açık kaynaklardan yararlanma teknikleri, bir takım disiplinleri içerir. İstatistik, veri madenciliği, makine öğrenimi, yapay sinir ağları, sosyal ağ analizi, sinyal işleme, örüntü tanıma, optimizasyon yöntemleri ve görselleştirme yaklaşımları bu tekniklere dahil edilebilir. Bilgi edinme alanında çok aşamalı bir büyüme modeli kullanılmaktadır. Bu model;

- Problem teşhisi,
- Literatür incelemesi,
- Araştırmanın tespiti,
- Bilimsel yöntem ile deneyler,
- Araştırmacı problemlerinin yanıtlanması olarak verilebilir.

Bilginin doğru bir şekilde kullanılmasıyla, bu süreçler problemlere yardımcı olabilir. Bu dört bölümlü sistem, bilgi keşfini desteklemek için kanıtlar bularak sonuçları doğrulamaya çalışır. Kanun uygulamasında, bir kişinin suç işleyip işlemediğini veya suçlanması gerektiğine karar vermede bu sistem oldukça önemlidir.

OSINT üzerinden siber tehditlerin tespitini yapmak ve önlemek için, suç şebekelerinin topolojilerini tanımlamak gerekir [15]. Ayrıca gizli ağların şifreli bilgilerini kullanarak suç şebekelerinin yapısal konumu incelenmelidir. Tartışma forumlarında bireyleri bulmak için metin analizini ve sosyal ağ analizini birleştiren bir yöntem geliştirmek gerekmektedir. Sitede izlenen üyelerin gözlemlenen mesaj içeriklerine bakılarak çok benzer durumları standartlar oluşturulup bu standartlar temel alınarak bir yöntem geliştirilmelidir. Yine veri madenciliği teknikleri kullanılarak durum analizi yapılmalıdır. İstenmeyen postaları spam yapmak ve siber suçlu davranış bağlamında şüphelilerin yazı stilini modellemek için birleşik bir veri madenciliği çözümü sunulmalıdır. Veri Madenciliği, Metin Madenciliği ve Sosyal Ağ Analizi, siber saldırı tespitini OSINT üzerinden yapmak için kullanılan yöntemlerden başlıcalarıdır.

Veri Madenciliği: Kendini sürekli güncelleyen ve teknoloji ile değişime giren çevre koşulları, insanların sınırları aşarak ortadan kaldırması ve dünyayı gittikçe daha da küreselleştirmesi, farklılaşan pazarlama ve Ar-Ge yöntemleri veri kavramından çıkılarak bilgi kavramının önemini her geçen gün daha da artacak şekilde ortaya koymaktadır [16]. Açık ve anlaşılır olarak tanımlamak gerekir ise veri madenciliği, geniş kapsamlı veriler arasından bilgiye ulaşma, bilgiyi madenleme (mining) işidir. Bu çalışmada veri madenciliği sınırlara ayrılmıştır. Bu sınırlar suç ağları, aykırılık tespiti, kötü amaçlı yazılım etkinlikleri algılama ve siber terörizmdir.

- Suç ağları sınırı, suç soruşturması için soruşturma sürecini kolaylaştıran sezgisel durumlar, yorumlanabilir kanıtlar ve sohbet günlüklerinden veri toplamak için veri madenciliği ile doğal dil işleme tekniklerinin birleşik bir çerçevesidir.

- Anomali tespiti sınırı, bilgi madenciliği için tipik bir bulanık saldırı tespit senaryosunu tanımlamaktadır. Ayrıca bilgisayar ağlarının güvenlik açıklarını inceleyen gerçek zamanlı uygulamalardır. Temel olarak beklenen davranışa uymayan verilerdeki kalıpları ve yapıları bulmaktadır [17].

- Kötü amaçlı yazılım etkinliklerini algılama, veri madenciliği kullanarak tespiti içerir. Örnek vermek gerekirse iki sınıftaki veriler: Beyaz ve siyah listeler gibi sınıf ayrımı yapılmaktadır.

- Siber terörizm ağının sınırlarını bulmak için faktör kavram analizi yoluyla destekleyici bir çerçeve sağlamak Webden bilgi alma ve Web istihbaratında bilgi boşluklarını doldurma amaçlı kullanılmaktadır. Veri setleri bu tür sınırlarda çok değerlidir.

Metin Madenciliği: Metin madenciliği kavramı metni veri kaynağı olarak kabul eden veri madenciliği çalışmasıdır [16]. Diğer bir ifadeyle verilen metin olarak değerlendirilerek oluşturulmuş (structured) veri elde etmeyi amaçlar. Karşı siber saldırı ve saldırı tespit sistemi olarak iki sınır belirlenmiştir [18]. Bu sınırlar ile metin madenciliği üzerinden elde edilen veri anlamlaştırılarak yöntem geliştirilmektedir.

- Karşı saldırı özellikle DDOS saldırısı benzeri saldırıları engellemek için kullanır.

- Saldırı tespit sisteminde, ağ sistemindeki cihazların güvenliğini sağlamak, yetkili olmayan kişilerin sistemlere girip bilgileri ele geçirmelerini veya değiştirmelerini engellemek için kimlik doğrulama ve erişim kontrolü gibi güvenlik mekanizmaları geliştirilmiştir. Bu anlamda saldırı tespiti yapabilmek için metin madenciliği ile sınırlar belirlenmelidir.

Sosyal Ağ Analizi: Sosyal ağ analizi, insani toplulukların yapısal içeriğini ağ ve çizge teorileri üzerinden değerlendiren analiz türüdür [19]. Bu analiz belirli ağ algoritmaları üzerinden sınıflandırma yaparak ağ sistemini grafiklere dökerek hangi düğümün belirlenmesi gerektiğini tespit eder. Ayrıca karşılaştırma yaparak en önemli düğüm tespit edilir [20]. Bu en önemli düğüm tespiti çeşitli ağ algoritmaları kullanılarak hesaplanmaktadır.

- İçeri-Derece Merkezliliği (In-degree centrality): Ağ içerisinde en çok etkileşimi alan düğümü öne çıkaran algoritmadır.

- Dışarı-Derece Merkezliliği (Out-degree centrality): Bu yöntem içerisinde içeri-derece merkezliliğinin aksine diğerleriyle daha fazla ilişki kuran düğüm öne çıkarak önem kazanır.

- Arasındalık Merkezliliği (Betweenness centrality): Ağ içerisindeki ilişkilerin en ortasında yer alan, bir diğer deyişle ayrıtların en kısa yoldan üzerinden geçtiği düğüm en önemli noktadır.

- Özvektör Merkezliliği (Eigenvector centrality): Özellikle sosyal medya analizlerinde en öne çıkan mimarilerden birisidir. Esasen, en çok etki sahibi olan, kurulan ilişkinin en önemli olduğu düğümü öne çıkarır. Bir sosyal ağdaki kanaat önderlerini öne çıkarmak açısından gereklidir.

C. SİBER SUÇ SORUŞTURMA ÇERÇEVESİ

Bu çalışma, siber suç soruşturmaları için açık kaynak verilerinin kullanılmasına yönelik mevcut çabaları gözden geçirmektedir [21]. Elde edilen her veri istihbarat açısından bilgi değildir [22]. Bu verilerin bir sistem mimarisi kurularak soruşturma çerçevesinden geçirilmesi gerekir. Şekil 2'de bulguların bütünleştirici yapısını yani siber suç soruşturma çerçevesi şeklinde bir özetini sunmaktadır.

Bilgi toplamanın ardından süreç değerlendirilir. Analizi süreç doğrultusunda yapılır ve gerekli yerler ile paylaşılır [23]. Geri bildirim ile soruşturma çerçevesi genişletilir.

Şekil 2. *Siber Suç Soruşturma Çerçevesi*

Siber suç soruşturma çerçevesi birkaç kısım bir araya getirilerek sağlanabilir. Siber saldırıda kullanılan araçlar ve teknikler hedeflenen sistem organizasyonunun kurumsal profilini etkilemeyecek şekilde yapılandırılmalıdır. Sistemimizdeki hedefler doğru belirlenmelidir. Siber saldırıların alan veya türü doğru tespit edilmelidir [24].

Bir diğer önemli kısım ise saldırıyı algılama ve önleme araçlarıdır. Algılama araçları ve teknikleri açık kaynak toplama, depolama ve ön değerlendirme yapmalıdır. Siber saldırılardan korunması gereken alanlar öncelikli sıraya göre değerlendirilmelidir [25]. Siber alanı korumak için açık kaynak toplama, depolama, analiz ve işleme stratejileri geliştirilmelidir. Bütün bu yapılanma açık kaynakların çeşitlendirilmesi ile güçlendirilmelidir [26].

V. OSINT KAVRAMININ DESTEK YÖNTEMLERİ

Siber suçun giderek artan etkisi, siber tehditlerin üstesinden gelmek için dünya çapında istihbarat ve kanun uygulayıcı kurumları gerektirdi. Şu anda tüm sektörler siber suçla en iyi şekilde nasıl mücadele edileceği ve güvenlik ile insanlara ve örgütlere nasıl etkili bir şekilde teşvik edileceğine ilişkin benzer ikilemlerle karşı karşıya kalmaktadır. Belirli hedeflerin kapsamlı bir profilini oluşturmak için açık kaynak kayıtlarını toplayarak benzersiz ve yüksek değerli istihbarat elde etmek, istihbarat topluluğu için önemli bir araç olarak hızla gelişmektedir. Mevcut açık kaynakların miktarı hızla arttıkça, siber suçla mücadelenin artması, bilginin etkili ve verimli bir şekilde toplanması ve işlenmesi için gelişmiş yazılımlara ve yöntemlere bağlıdır. Bütüncül bir OSINT yapısı geliştirerek siber suça karşı yapılan araştırmalar için açık kaynak verilerinin kullanılmasına yönelik mevcut çabaların gözden geçirilmesi gerekmektedir

OSINT mantığında bazı teknikler ya da metotlarda yukardaki tekniklere destek olarak siber savunmada etkili şekilde kullanılabilir. Siber suç soruşturma destek yöntem ve modellerinin sınıflandırılmasını yapmak gerekirse önde gelen yöntemler: Madencilik Teknikleri, Analiz Teknikleri, İstatistiksel Metotlar ve OSINT Yöntem Kolaylaştırmasıdır.

A. MADENCİLİK TEKNİKLERİ

Sosyal medya siteleri tüm dünyada milyarlarca insanın ürettiği her çeşit bilgiyi depolamaktadır. Depolanan bu verilerden ortaya çıkan büyük veri (Big Data) kelimesi son yıllarda hızlı hayatımıza giren bir kavramdır. İşte tam bu noktada madencilik teknikleri, büyük veride bilgiyi elde etme yöntemlerinden biridir. İnternet ortamındaki binlerce veri belirli enformasyon teknikleri ile bilgi haline çevrilir. Bu sebeple güvenlik için yeterli miktarda bilgi elde edilmelidir [27]. Çünkü bu bilgiler güvenlik anlayışı için oldukça gereklidir [28]. Bu sayede OSINT kavramı veri madenciliği yöntemleri ile internet ortamındaki karmaşık ve anlamsız verilerden anlamlı verileri oluşturur. Madencilik teknikleri olarak en sık kullanılan teknikler sırasıyla;

- Veri Madenciliği: Çok büyük verilerde bilgiye ulaşma işidir.
- Metin Madenciliği: Metinler üzerinden bilgi ortaya çıkarma ve sınıflandırma işidir.
- Optimizasyon Yöntemi: Elimizdeki bilgi kaynaklarından istihbarat bilgisini elde etme işidir.
- Web Madenciliği: İnternet üzerindeki bilgileri işleyerek analiz etmektir.
- Makine Öğrenmesi: Sayısal öğrenme ve model tanıma işlemidir.

B. ANALİZ TEKNİKLERİ

İstihbarat açısından analizin en temel amacı internet ağ ortamındaki suç ilişkilerini ortaya çıkartmaktır. Sosyal ağ analizi öncelikle toplumun birbiriyle nasıl ilişki kurduğu ile ilgili bir yöntemdir. Kim nerede, ne zaman, kimle, nasıl ve ne yapıyor mantığı ile çalışır [29]. Beğenilen resimlerden paylaşılan müziklere kadar detaylı incelemeler yapan bir tekniktir [30]. Analiz teknikleri açısından sosyal ağ analizi ele alınırsa insanların koloni halindeki yapılarını ağ ve çizge teorileri üzerinden değerlendirerek analiz eder [31]. Bu yöntemler çerçevesinde açık kaynak istihbaratı elde etmek sosyal ağ analizi ile mümkündür. Analiz teknikleri aşamalı olarak 3 başlık altında toplanabilir;

- Görevlendirme: Sosyal ağlarda inceleme yapılırken analizin detayları planlanmalıdır.
- Sayısal Değerlendirme: Açıkça ağdaki bilgilerin sayısal olarak değerlendirmesidir.
- Veri Toplama: Sosyal medyadaki tüm kaynakların veriden bilgiye dönüşmesi için veri toplama işidir.

C. İSTATİSTİK METOTLARI

İstatistik metotları, açık kaynak üzerinden yapılan istihbarat araştırmasında çözüm elde etmek için varılan sonuçların alt problemlere bölünerek sonuca vardırılması yöntemidir. İstatistiki metotlar kişiler arasındaki ilişkinin belirli yöntemler eşliğinde ortaya çıkarılması için kullanılır. Bunlar sırasıyla;

- Regresyon Modelleri: Kişilerin değişken olarak kabul edilerek davranışların modeller üzerinden tespiti ve tahminidir.

- Sayısal Veri Toplama: İnternetin sayısal dünyasının değerleri olan arama, satın alma veya paylaşma türündeki işlemlerin ortaya çıkarttığı verilerdir.
- Özetleme Yöntemleri: İstihbarat bilgilerinin grafikler ve tablolar üzerinden kümelenme yöntemidir.

- Analiz Etme Yöntemleri: Bilgilerin istatistik değerlerine ulaşmak için detaylandırma sistemidir.

- Yorumlama Yöntemleri: İstatistiklerin analiz edilerek istihbarat çerçevesinde yorumlanmasıdır.

D. OSINT YÖNTEMİ KOLAYLAŞTIRMASI

Yöntemin kolaylaştırılması OSINT kavramını oluşturmayı kolaylaştırmak ve modern dünyanın temel sorunlarına yanıt olarak araştırmaları çevrimiçi yapmak için tasarlanmış çözümlemelerdir [32]. Bu yöntemler çevrimiçi iyileştirme ve tesir etme, ulusal güvenlik ve savunma ile çevrimiçi suç kavramlarının bir araya gelerek oluşturduğu teknik çözümlerdir.

Çevrimiçi İyileştirme ve Tesir Etme: OSINT Yöntemi Kolaylaştırma tekniklerinden ilki olan çevrimiçi iyileştirme ve tesir etme, internet ortamında saldırgan profili çizen bireylerin ve aktivistlerin belirlenmesi ile başlar. Aktif ve pasif saldırı yapabilecek kişilerin ağlarda aktif koklama (sniffing) yapılarak gerçek zamanlı olarak izlenmesi yöntemi ile devam eder. Bu izlemeler sonucu elde edilen bilgiler internette bilgi yayımı ve bildirimler ile gerekli haber kaynaklarına ulaştırılır. İstihbarat birimleri kendi aralarında haberleşerek kritik kurumları uyarır. Kritik kurumlar halka gerekli bilgilendirmeleri yapar. Bu çerçevede halkın tutumu sunulan bu bilgiler ışığında gerekli araçlar ile takip edilerek OSINT bilgiler elde edilir. Çevrimiçi iyileştirme sağlanarak gerekli yöntemler en başa dönülerek tekrar OSINT analizi için tarama yapmaya devam eder.

Ulusal Güvenlik ve Savunma: Ulusal güvenlik ve savunma tekniği ulusal kurum ve kuruluşlara yönelik tehlikeleri belirlemek amaçlı bir yöntemdir. Kurumlar arasında gerekli işbirliği sağlanarak istihbarat ile alınacak tedbirler ışığında ortak elde edilen verilerdir. Ulusal güvenliğin sağlanarak gerekli savunmanın yapılması için terör örgütlerinin belirlenmesi ve araştırılması, uyum ve yaptırımlar gerçekleştirilmesi, saldırgan yapıların internetteki açık bilgilerin keşfedilerek analizlerinin yapılması, saldırgan hedeflerin coğrafi lokalizasyonunun yapılması ve askeri operasyonlar için OSINT kaynakları sağlanması için kullanılan yazılımsal ve donanımsal araçları içermektedir.

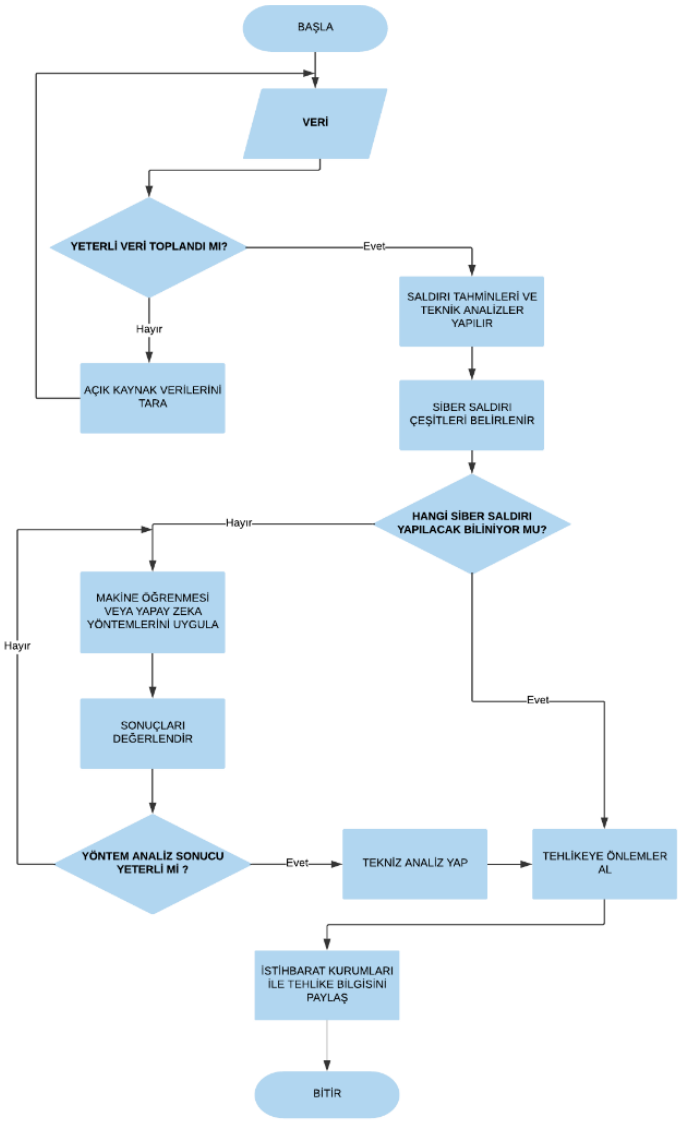
Çevrimiçi Suçlar: Yukardaki yöntemlerin dışında belirli sorular belirlenerek açık kaynak istihbaratı elde etmek destekleyici bir tekniktir. Bu sorulardan bazıları sırasıyla;

- Kuruluşunuza kim saldırıyor?
- Amaçları nelerdir?
- Nasıl örgütleniyorlar?
- Kullandıkları araçlar nelerdir?

Soruların cevapları detaylı analiz edilerek diğer yöntemler ile birleştirilmektedir. Bu soruların cevapları arasındaki ilişkiyi analiz etmek gerekmektedir. Ülkeler ve kuruluşlar üzerinden ticari amaçlı veya toplumsal güvenlik açısından siber istihbarat yapılarının sosyal medya üzerine yoğunlaşmaları gerektiği anlaşılmaktadır. Çünkü sosyal medya günümüzde, sanalın gerçeğe dönüşmesini sağlamaktadır. Bu açıdan sosyal medya gerçek hayatın tamamen kendisi haline dönüşmeye başlamıştır. Bu yüzden Facebook ve Twitter gibi sosyal ağlardan bilgi toplanmalıdır [33]. Ayrıca belirli içerik ve etkinlikler için internette arama yapılmalıdır. İnternetten elde edilen bilgileri kanıtlar haline getirilip tanımlama şekline dönüştürülmesi gerekmektedir. Özet olarak, OSINT alanı için teknik ve metotlar geniş bir yelpazeyi içermektedir [34,35].

VI. OSINT İLE SİBER SALDIRI TEHDİT ALGORİTMASI

Çeşitli kaynaklarda açık halde bulunan verilerin toplanarak süzgeçten geçirilmesi ve istihbarat bilgisi elde edilmesi bu makalede önerilen bir algoritma ile sağlanmaktadır. Açık kaynaklardaki veriler toplanarak bilgiye dönüştürülmesi ve bilgininde istihbarat değeri taşıdığı kararı ulaşılmak istenilen sonuçtur. Gerekli işlemler algoritma çerçevesinde adım adım belirtilmektedir. Önerilen algoritmanın yeterli veri toplanması kararı sonrası önceden belirlenen teknik analizler için ilgili sisteme gönderilmektedir. Sistem bu analiz sonucunda kendi veri tabanını kontrol ederek saldırının istihbarat kurumlarınca bilenen bir siber saldırı olup olmadığını kontrol etmektedir. Eğer verilerden elde edilen istihbarat bilgileri çeşitli sonuçlar üretiyorsa kestirim yapmak zorlaşmaktadır. Bu adımda makine öğrenmesi veya yapay zeka yöntemlerinden birkaç tanesini uygulayarak en ideal olan sonucu üretmektedir. Bu süreç çeşitli uygulamalar üzerinden en etkili makine öğrenmesi veya yapay zeka yöntemi ile analiz edilinceye kadar devam etmektedir. Makine öğrenmesi uygulamaları sonucunda en yüksek tahmine göre teknik analizler yapılır. Tehlikeye karşı gerekli önlemler alınır. İstihbarat kurum ve kuruluşları ilgili alanda bilgilendirilir. Önerilen algoritma Şekil 3`te gösterilmektedir.



Şekil 3. *OSINT ile Siber Saldırı Tehdit Algoritması*

VII. SONUÇLAR

Siber suçun etkisi, siber tehditlerin üstesinden gelmek için dünya çapında istihbarat ve kanun uygulayıcı kurumlar gerektirmektedir. Gerek devlet kurumları gerekse özel kurumlar açısından tüm sektörler şu anda siber suçları en iyi şekilde nasıl hafifletilebilecekleri ile ilgili benzer ikilemlerle karşı karşıya kalmaktadır. Belirli hedeflerin kapsamlı bir izlenimini oluşturmak için açık kaynak kayıtlarını toplayarak benzersiz ve yüksek değerli istihbarat elde etmek, istihbarat topluluğunun önemli bir aracı olarak hızla gelişmektedir. Bu makalede siber suç soruşturma çerçevesinde uygulanan algoritma ile istihbarat verileri adım adım incelenmiştir. Elde edilen bilgiler açık kaynak istihbaratı çerçevesinde değerlendirilmiştir.

Mevcut açık kaynakların miktarı hızla arttıkça, siber suçla mücadelenin artması, bilginin etkili ve verimli bir şekilde toplanması ve işlenmesi için gelişmiş yazılım araçlarına ve tekniklerine bağlıdır. Bu çalışmada OSINT kavramının siber suçla mücadelede nasıl kullanılacağı gerekli yöntem ve teknikler

eşliğinde açıklanmıştır. Açık kaynak istihbaratının çerçevesi belirlenmiştir ve yöntemlere ayrılarak açıklanmıştır.

VIII. KAYNAKLAR

[1] M. Roozbehani, A. Povilionis, C. Schunck ve M. Talamo, "On the Fragility of Network Security Verification in Rare-Observation Regimes," *IFAC-PapersOnLine*, vol. 50, no.1, pp. 411-418, 2017.

[2] M. Glassman ve M. J. Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior*, vol. 28, no. 2, pp. 673-682, 2012.

[3] C. Hobbs, M. Moran ve D. Salisbury, *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, Springer, 2012.

[4] R. A. Best Jr ve A. Cumming, "Open source intelligence (OSINT): Issues for congress," Congressional Research Service Reports, Rap. 5 Aralık 2007.

[5] PWC cyber security, (16 Ocak 2019). [Online]. Erişim: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[6] O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue ve J. Spiegel, "The Law of Cyber-Attack," *California Law Review*, vol. 100, pp. 817-885, 2012.

[7] R. Layton, C. Perez, B. Birregah, P. Watters ve M. Lemercier, "Indirect information linkage for OSINT through authorship analysis of aliases," *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, Gold Coast, Avustralya, 2013, pp. 36-46.

[8] A. S. Hulnick, "The dilemma of open sources intelligence: Is OSINT really intelligence?," *The Oxford Handbook of National Security Intelligence*, New York, A.B.D: Oxford University Press, Inc., 2010.

[9] D. Quick ve K. K. R. Choo, "Digital forensic intelligence: Data subsets and open source intelligence (DFINT+ OSINT): A timely and cohesive mix," *Future Generation Computer Systems*, vol. 78, pp. 558-567, 2018.

[10] G. Hribar, I. Podbregar, ve T. Ivanuša, "OSINT: a "grey zone"?," *International Journal of Intelligence and CounterIntelligence*, vol. 27, no. 3, pp. 529-549, 2014.

[11] S. A. Stottlemyre, "HUMINT, OSINT, or something new? Defining crowdsourced intelligence," *International Journal of Intelligence and CounterIntelligence*, vol. 28, no. 3, pp. 578-589, 2015.

[12] J. M. Carroll, "OSINT analysis using adaptive resonance theory for conterterrorism warnings," *Artificial Intelligence and Applications*, pp. 756-760, 2005.

[13] N. Einwechter. (7 Ocak 2002). *An introduction to distributed intrusion detection systems*. Erişim: https://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems.

[14] L. Benes, "OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm," *Journal of Strategic Security*, vol. 6, no. 5, pp. 22-37, 2013.

[15] Y. Benkler ve H. Masum, *Collective Intelligence: Creating a Prosperous World at Peace*, Oakton, Virginia, A.B.D.: Earth Intelligence Network, 2008.

[16] F. Schaurer ve J. Störger, "The evolution of open source intelligence (OSINT)," *The Intelligencer Journal of U.S. Intelligence Studies*, vol. 19, pp. 53-56, 2013.

[17] M. Vigil, J. Buchmann, D. Cabarcas, C. Weinert ve A. Wiesmaier, "Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey," *Computers & Security*, vol. 50, pp. 16-32, 2015.

[18] R. D. Steele, "Information peacekeeping: The purest form of war," *Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated*, Carlisle Barracks, A.B.D.: U.S. Army War College Strategic Studies Institute, pp. 143-171, 1998.

[19] N. D. Thuc, N. C. Phu, T. N. Bao ve V. T. Hai, "A Sofware Solution for Defending Against Man-in-the-Middle Attacks on Wlan," Department of Electronic Engineering and Information Sciences, Ruhr University Bochum, Germany, 2015.

[20] S. Gong, C. Jaeik, ve L. Changhoon, "A Reliability Comparison Method for OSINT Validity Analysis," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 12, pp. 5428-5435, 2018.

[21] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta ve Q. Wu, "AVOIDIT: A cyber attack taxonomy," *In Proc. of 9th Annual Symposium On Information Assurance-ASIA*, 2009 vol. 14, pp. 12-22.

[22] B. J. Koops, J.H. Hoepman, R. Leenes, "Open-Source Intelligence and Privacy by Design," *Computer Law & Security Review*, vol. 29, no. 6, pp. 676-688, 2013.

[23] A. S. Hulnick, "The Downside of Open Source Intelligence," *International Journal of Intelligence and CounterIntelligence*, vol. 15, no. 4, pp. 565-579, 2010.

[24] E. Otte ve R. Rousseau, "Social Network Analysis: A Powerful Strategy, Also for the Information Sciences," *Journal of Information Science*, vol. 28, no. 6, pp. 441-453, 2002.

[24] F. Stalder ve J. Hirsh, "Open source intelligence," *First Monday*, vol. 7, no. 6, 2002.

[25] C. Best, "OSINT, the internet and privacy," *2012 European Intelligence and Security Informatics Conference*, Odense, Denmark, 2012, pp. 4.

[26] S. Mittal, P. K. Das, V. Mulwad, A. Joshi ve T. Finin, "Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities.," *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, San Francisco, CA, USA, 2016, pp. 860-867.

[27] L. K. Johnson, (Ed.)., *Handbook of Intelligence Studies*, 1. Baskı, New York, A.B.D.:Routledge, 2007.

[28] R. Vatrapu, R. R. Mukkamala, A. Hussain ve B. Flesch, "Social Set Analysis: A Set Theoretical Approach to Big Data Analytics," *IEEE Access*, vol. 4, pp. 2542-2571, 2016.

[29] G. Cascavilla, F. Beato, A. Burattin, M. Conti ve L. V. Mancini, "OSSINT-Open Source Social Network Intelligence an Efficient and Effective Way to Uncover" Private" Information in OSN Profiles," *Online Social Networks and Media*, vol. 6, pp. 58–68, 2018.

[30] H. Zhang, R. Dantu ve J. W. Cangussu, "Socioscope: Human Relationship and Behavior Analysis in Social Networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 41, no. 6, pp. 1122-1143, 2011.

[31] S. Wasserman ve K. Faust. "*Social Network Analysis: Methods and Applications*," Cambridge, U.K.: Cambridge Univ. Press, pp. 505–555, 1994.

[32] S. Noubours, A. Pritzkau ve U. Schade, "NLP as an essential ingredient of effective OSINT frameworks," *IEEE Military Communications and Information Systems Conference*, Canberra, Avustralya, 2013, pp. 1-7.

[33] M. A. Pravia, R. K. Prasanth, P. O. Arambel, C. Sidner, ve C. Y. Chong, "Generation of a fundamental data set for hard/soft information fusion," *IEEE 11th International Conference on Information Fusion*, Köln, Almanya, 2008, pp. 1-8.

[34] D. Bradbury, "In plain view: open source intelligence," *Computer Fraud & Security*, vol. 4, pp. 5-9, 2011.

[35] R. D. Steele, "Open source intelligence," *Handbook of Intelligence Studies*, Routledge, 2007, pp. 129-147.