Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme

Öğr . Gör. Yeliz ŞENKAYA*, Arş. Gör. Uğur Güven ADAR**
* Ordu Üniversitesi Bilgi Yönetimi Bölümü, Ordu
yelizsenkaya@hotmail.com
**Atatürk Üniversitesi Bilgisayar Mühendisliği Bölümü, Erzurum
ugur.adar@atauni.edu.tr

***Özet*— Siber saldırı; dünyanın herhangi bir yerindeki bilgisayar kontrolü altındaki sistemlere internet (sanal) ortamından izinsiz erişip kritik alt yapının yönetimini ele geçirmeye çalışmaktır. Siber saldırının silahları ise internet ortamına bağlı bir bilgisayarın tuşları, bu tuşlara dokunan parmaklar ve yazılımlardır[1]. Etkin ağlarda siber saldırı ile tüm alt yapılar bir anda yerle bir edilebilir, en güçlü ülke bile hareket edemez hale getirilebilir. Etkin ağlarda dinamik olarak gelişen saldırılara karşı savunmak için geleneksel sabit algoritmalar ile yazılım geliştirmek güçtür. Bu durum, yazılım esnekliği ve öğrenme yeteneği sağlayan yapay zeka yöntemleri uygulanarak ele alınabilir. Bu yayında siber saldırılara karşı alınacak akıllı siber savunma yöntemlerinden bahsedilmiştir, siber savunmada kullanılan zeki yöntemlerden en çok dikkat çekenler daha kapsamlı araştırılmıştır. Diğer taraftan, birçok siber savunma sorununun sadece yapay zeka kullanılarak başarıyla çözülebileceği görülmüştür. Dünyada yapılan siber saldırılara ilişkin örnekler verilmiştir.**

Anahtar Kelimeler: Siber saldırı, siber savaş, siber savunma, akıllı siber savunma yöntemleri, siber savunmada yapay sinir ağları, siber savunmada uzman sistemler

I. GİRİŞ

Bilgi çağını yaşadığımız şu günlerde, e-devlet, e-imza, e-ticaret gibi kavramlardan oldukça sık bahsedilmektedir. Gerek hız ve verimlilik artışı, gerekse kolaylık sağlaması nedeniyle birçok bilgi elektronik ortamlara aktarılmıştır. Ancak, kişisel veya kurumsal açıdan önemli bir bilginin, başkalarının eline geçmesi ile maddi ve manevi zararlara yol açabileceği görülmüştür. Geliştirilen e-devlet, e-kurum gibi projelerde güvenliğin en üst düzeyde tutulması ulusal bir amaç haline gelmiş, bu konuda hukuki ve teknolojik önlemler geliştirilmiştir[2].

Her şeyin bu kadar sanal ortamda gerçekleştiği şu günlerde siber savaştan söz etmemek imkansızdır. Siber savaşı açıklamak gerekirse; düşmanı psikolojik olarak çökertmek için bilgisayar kontrolü altındaki sistemlerine izinsiz, gizli ve görünmez olarak internet üzerinden erişmektir. Kontrolü ele geçirerek bilgileri çalmak, değiştirmek, çökertmek ya da yanlış yönlendirmektir[1]. Komplo teorileri ya da efsane gibi anlatılan siber savaş senaryoları günümüzde gerçek olmaya başlamıştır. İnternet üzerinden yapılan siber saldırılar artık önemsenmesi gereken ciddi bir tehlikedir. Hava, kara, deniz ve uzaydan sonra savaş artık sanal dünyaya taşınmıştır. Siber ortamdaki aktivasyonlar siber saldırı, siber silahlar, siber savaş ve siber savunma(CD) olarak adlandırılmakta, kısaca 4S olarak tanımlanmaktadır.

Zamanımızın düşmanı hareketsiz, erişilmez ve ulaşılmazdır. Düşmanlarımız yakınımızda ya da karşımızda olmayacaktır. Görülmez, bilinmez ve anlaşılmaz olduklarından siber saldırılar fiziksel saldırılardan çok daha tehlikelidir. Bilgisayar sistemlerindeki yazılımları ve kodları devre dışı bırakmak, çalmak, yok etmek, bozmak, kendi amaçları doğrultusunda çalıştırmak için yapılan siber saldırılarda artış görülmektedir.

II. SİBER SAVUNMA

İnternetin ve iletişim olanaklarının artmasıyla birlikte saldırganlar tarafından saldırılabilecek daha çok sistem ortaya çıkmıştır. Bu saldırıların büyük bir bölümü kullanılan sistemin kusurları veya eksiklerinden faydalanılarak yapılır. Bu tür saldırıları engellemenin iki yolu vardır; ilki tamamen güvenli bir sistem ve ortam oluşturmak, ikincisi ise saldırıları tespit edip gerekli önlemleri almaktır. Bunlardan ilki pratik açıdan mümkün olmamaktadır. Bunların gerekçeleri ise [3],

- Kullanılan işletim sisteminde var olan açıkların genellikle ilk olarak saldırganlar tarafından fark edilmesi ve önlem alınana kadar bu açıkların kullanılabilmesi,
- Veri iletiminde kullanılan protokollerin yapısında var olan bazı kuralların saldırı amaçlı kullanılabilmesi,
- Kriptografik metotların ve anahtarlarının kırılabilmesi, kullanıcıların şifrelerini unutabilmesi

veya kripto-sistemin kırılabilmesi gibi nedenlerle yüksek seviyede bir güvenlik sağlanamaması,

- Dış ortama karşı güvenliği sağlanan sistemin, iç ortamlardan suistimal edilerek güvenliğin ortadan kaldırılması,
- Güvenlik amacıyla kullanıcı yetkilerinin minimuma indirilmesi sonucu kullanıcı verimliliğinin düşmesi gibi nedenleri vardır.

Sistemlerini korumak isteyenler, genelde saldırı gelene kadar bekleme pozisyonunda kalmak, saldırı geldiğinde ise olabildiğince hızlı tespit etmek isterler. Bu ise siber savunma'nın yaptığı iştir . Bir saldırının hangi adresten veya hangi porttan geldiğini bilmeden engel olmak mümkün değildir. Siber savunma teknikleri ile saldırıları tespit ederken bu bilgileri de elde ederler.

Yapay zeka ile oluşturulan Siber savunma teknikleri detaylı olarak topladığı ve depoladığı bilgilerden yararlanarak, saldırıları olabildiğince erken tespit etme özelliğine sahiptir. Yine aynı bilgilerin incelenmesi ile daha önce hiç karşılaşılmamış bir saldırıyı da tespit edebilir. Siber savunmada yapay zekayı cazip hale getiren bu özelliktir.

III. YAPAY ZEKA

Yapay Zeka denilince ilk olarak insanın aklına insan gibi düşünebilen yada onu taklit edebilen veya bir beynin klonlanması anlamında düşünülmektedir. Bilgisayarların kişileştirilmesi akla gelmektedir. Oysa bizim araştırmakta olduğumuz yapay zeka kavramını çeşitli problemler çözerken yararlandığı algoritma yapısını bir insanın problem çözme mantığı ile bağdaştırmaktır. Yapay zeka kabaca; bir bilgisayarın ya da bilgisayar denetimli bir makinenin, genellikle insana özgü nitelikler olduğu varsayılan akıl yürütme, anlam çıkartma, genelleme ve geçmiş deneyimlerden öğrenme gibi yüksek zihinsel süreçlere ilişkin görevleri yerine getirme yeteneği olarak tanımlanmaktadır [4]. Genel bir tanımlama yapmak istersek davranışları insan gibi olan bilgisayar sistemleri yapmak amaçtır. Yapay zeka kavramında önemli olan bilgidir. Bilgiden sonuç üreterek bunu bir nedene bağlaması ise düşünebilmesine yapay zekasının örnek olarak gösterilebilir. Tabi ki bunları gerçekleştirirken konusunda üst düzeyde veriden çok bilgi sahibi olması beklenir. Bilgileri birleştirir, analiz eder, sonuca varır ve bu sonucu ise bir nedene bağlar.

Yapay Zeka kavramının geçmişi modern bilgisayar bilimi kadar eskidir. Fikir babası, "Makineler düşünebilir mi? " sorusunu ortaya atarak Makine Zekasını tartışmaya açan Alan Mathison Turing'dir. Yapay zekanın insan gibi düşünmesine geri dönersek, verebileceğimiz en uygun örnek Rus Satranç Şampiyonu Kasparov'u yenen bir yapay zeka (DeepBlue)nın üretilmiş olmasıdır. Bilgisayarın başlangıç günlerine dönecek olursak bir yapay zekânın satranç oyunu oynayarak, dünya şampiyonunu yenebilecek olması neredeyse imkânsız gibi görünüyordu. Oysaki bu gerçekleşti. Bunun 3 nedeni vardır: artırılmış bilgisayar gücü, iyi bir algoritma ve tüm mümkün satranç bilgilerini içeren iyi planlanmış bilgi tabanlarının olmasıdır.

Aslına bakarsak, satranç problemi çözülebilirdi çünkü o narrow AI diye adlandırılan özel zeka problemiydi. Diğer bir durum ise General AI gerektiren bir dilden başka dile çeviri. Geçen yüzyılın 60larında,özellikle N.Chomski'nin yapısal dilbilim alanındaki çalışmalarından sonra, yakınlarda olağan dil çevirme probleminin çözüleceği düşünülüyordu. Google' ın AI dilbilimi gibi bazı özel uygulamalarda başarı görünebilir olsa bile, henüz bu gerçekleşmedi. Sebep bunun insan aktiviteleri ile alakalı tüm alanlarda çok miktarda bilgiye sahip olunması ve bunlarla başa çıkabilecek general yapay zeka istemesidir.

IV. SİBER SAVUNMADA YAPAY ZEKAYA NEDEN İHTİYAÇ VARDIR?

Öncelikle size Conficker solucanından bahsetmek istiyorum. Avrupa da ki askeri ve polis ağlarında Conficker 'in bazı etkileri şunlardır: [5]"Intramar Fransız donanması bilgisayar ağına 15 Ocak 2009 tarihinde Conficker bulaştı. Ağ daha sonra karantinaya alındı, başka bilgisayarlara virüs bulaşmasın diye. İngiltere Savunma Bakanlığı bazı büyük sistemlerine ve masaüstlerine virüs bulaştığını bildirdi. Virüs idari ofislere yayıldı, çeşitli kraliyet savaş gemilerine ve kraliyet donanması denizaltı gemisinde *Nawystar/N masaüstüne ve Sheffield şehir genelindeki hastanelerde 800'ün üzerinde ki bilgisayarlarda virüs bildirildi. Bundeswehr, Federal Almanya Cumhuriyetinin silahlı kuvvetlerinin yaklaşık yüz bilgisayarında virüs olduğu bildirildi.2010 Ocak ayında, Manchester polis ağına virüs bulaştı, bir tedbir olarak 3 gün süreyle ulusal polis bilgisayarlarıyla iletişim kesildi. Bu süre içerisinde, rutin denetimleri yapmak için subay araçlar ve insanları denetlemek zorunda kalmıştır! "

İşte artış gösteren bu siber saldırılara karşı teknolojik önlemlerin geliştirilmesi sırasında bir varlık olarak bilgiyi, tehdit ve saldırılara karşı korumak için siber savunma yöntemleri geliştirilmiştir. Ancak akıllı siber silahlarına karşı savunma sadece akıllı yazılımla elde edilebilir.

Yukarda bahsettiğim Conficker virüsü gibi olayların tekrar yaşanmaması için acilen siber savunma değişikliklerine ihtiyaç vardır. Yeni savunma yöntemleri güvenli bir ortam, kapsamlı durum farkındalığı , ağlardaki saldırılara son derece otomatik tepki veren yapay zeka yöntemleri ve bilgi tabanlı araçların geniş kullanımını gerektirir.

Neden siber operasyonlarda akıllı yazılımın rolü çok hızlı artmıştır? Siber uzaya yakından baktığımızda, cevabı görebilirsiniz. Yapay zeka , internet durumlarına öncelikle her şeyden önce tepki verdiği için gereklidir. Siber uzayda olaylara çok hızlı tepki verdiği, olayları analiz ettiği ve gerekli kararları aldığı için yapay zeka gereklidir. Etkili bir siber uzayda saldırılara karşı savunmak için geleneksel algoritmalar ile yazılım geliştirmek güçtür. Çünkü yeni tehditler sürekli

ortaya çıkar. Bu yüzden yapay zeka yöntemlerini kullanmak gerekir.

V. SİBER SAVUNMADA KULLANILAN ZEKİ SİSTEMLER

Bilgisayar veya ağ sistemlerine yapılan saldırıları tespit ederek güvenliğin sağlanması için geliştirilen CD metotları, her ne kadar yapılan saldırıların büyük bir çoğunlunun tespit edebilseler de daha önce hiç karşılaşılmamış olan saldırıların büyük çoğunluğunun tespit edilememesi ve bu saldırıların sistemlerde büyük zararlara yol açması, yeni saldırı çeşitlerinin tespit edilebilme başarısının artırılması ihtiyacını getirmiştir. Bu ihtiyacın karşılanması ve hızla değişen saldırı tiplerinin karşısında, bilgi ve bilgisayar güvenliğinin sağlanması amacıyla, CD lerin geliştirilmesinde yapay zeka yöntemleri kullanılarak siber savunma performanslarının iyileştirilmesi hedeflenmiştir. Yapay zeka tekniklerinin öğrenilebilmesi hızlı hesaplama, genelleme matematiksel olarak modellenmesi zor olan problemlere çözüm sunabilmesi gibi özellikler, bu yaklaşımların siber savunmada kullanılmasının önemli gerekçelerindendir.

Zeki yaklaşımların kullanılmaya başlaması ile birlikte anormallik tespiti yaklaşımı biraz daha ön plana çıkmış ve bu sayede anormallik tespitinin yeni saldırıları tespit edebilme yeteneği arttırılmıştır. Yapay zeka araştırmacılarının baştan beri ulaşmak istediği ideal, insan gibi düşünen ve davranan sistemler geliştirmektir. Ancak buna ulaşmanın güçlüğü anlaşılınca çalışmanın yönü rasyonel düşünen ve davranan sistemlerin tasarlanmasına çevrilmiştir. Geleneksel yöntemlerle çözümü zor veya imkansız olan problemlerin çözümünde kullanılan yapay zeka teknikleri; neural nets, expert sistemler, intelligent agents, genetic algoritmalar, fuzzy logic, search, leraning olarak sıralanabilir. Bu söylediğim yapay zeka tekniklerinden göz atalım.

A. Neural nets(yapay sinir ağları)

Zeki yaklaşımların CD'lerde kullanılmaya başlaması, farklı birçok zeki yöntemin de kullanılabilir olduğunu göstermiştir. Bu tekniklerden hemen hemen hepsi CD da kullanılmış olsa da, elde edilen başarılı sonuçlardan dolayı en çok kullanılanlardan biri Yapay Sinir Ağı'dır(YSA) [6, 7]. Yapay sinir ağları: Giriş ve çıkışları olan birbirleri ile sıkı bir şekilde ilişkilenmiş işlem elemanları olup insan beynindeki hücrelerin çalışma prensibini modelleyen bir bilgisayar sistemidir.

YSA , Frank Rosenblatt'ın 1957'de icat ettiği Perceptron ile başlayan uzun bir tarihe sahiptir. YSA'nın en popüler elementlerinden biri olarak kalan sinirdir (neuron)[8]. Birleştirilen az sayıda perceptron hali hazırda öğrenebilir ve ilginç problemleri çözebilir. Fakat YSA çok sayıda yapay sinirden meydana gelebilir. Bu yüzden YSA, çok sayıda paralel öğrenme ve karar verme işlevi sağlar. En ayırt edici özellikleri işlem hızlarıdır. Öğrenme modeli tanıma[9], sınıflandırma, ve hamlelere cevap seçme, vb. özellikler için uygundur. Hem donanımda hem yazılımda kullanılabilir.

YSA, işgal saptama ve önlemede kolayca uygalanabilir. Onları DDoS saptamada[10], bilgisayar virüsü saptamada[11], istenmeyen e-postaları saptamada(spam)[12], zombie saptamada[13], kötü amaçlı yazılımları sınıflamada(malware)[14] ve hukuki soruşturmalarda kullanmaya yönelik teklifler olmuştur[15].YSA'nın siber savunmadaki popüleritesinin sebeplerinden biri , donanımda veya grafik işlemcide kullanıldıklarında, hızının yüksek olmasıdır.YSA teknolojisinde yeni gelişmeler vardır: üçüncü nesil neural ağlar- biyolojik nöronları (sinir) daha gerçekçi taklit eden YSA 'yı arttırır ve daha fazla uygulama fırsatı sunar.

B. Expert Sistemler (Uzman)

'Ancak bir uzman insanın çözebileceği karmaşık problemlerin bilgisayar ile çözümüne olanak sağlayan sistemler' denilebilir. Uzman sistemler bir yapay zeka programlamadır. Genel olarak bir algoritma kullanmazlar, önemli olan veritabanından çok bilgidir. Expert sistemler tartışmasız en çok kullanılan AI araçlarıdır. Bir expert sistemi, bir kullanıcı ya da yazılım tarafından gösterilen uygulama alanlarında sorulara cevap bulmada kullanılan yazılımlardır[16]. Direk olarak medikal tanılar, finans ya da cyberspace gibi alanlarda, karar desteklemede kullanılabilir. Expert sistemlerin, küçük teknik tanımlama sistemlerinden karmaşık problemleri çözmede kullanılan çok büyük ve teferruatlı hybrid(melez) sistemlere kadar birçok çeşidi vardır. Kavram olarak, bir expert sistem, belirli bir uygulama alanı ile ilgili uzman bilginin depolandığı bir bilgi tabanını içerir. Bilgi tabanının yanı sıra, bu bilgiye dayalı olarak cevap üreten çıkarsama motoru, ve tabi ki bir durumla ilgili ek bilgi içerir. Boş bilgi tabanı ve sonuç motoru birlikte Expert sistem kabuğu olarak adlandırılır- kullanılmadan önce bilgi ile doldurulmalıdır. Expert sistem kabuğu, bilgi tabanına bilgi eklemek için bir yazılımla desteklenmelidir, ve kullanıcı etkileşimi için programlarla ve hybrid expert sisteminde kullanılabilecek diğer programlarla desteklenebilir. Bir expert sistemi geliştirmek demek, ilk olarak bir expert sistem kabuğu seçimi/ adaptasyonu, ikinci olarak ise uzman bilgi edinip bilgi sistemini bilgi ile doldurmak demektir. İkinci adım, ilkinden daha karmaşık ve zaman alıcıdır.

Expert sistemleri geliştirmek için birçok araç vardır. Genellikle, bir araç bir expert sistem kabuğu içerir ve aynı zamanda bilgi havuzuna bilgi ekleyecek işleve de sahiptir. Expert sistemler simülasyon, hesap yapma gibi işlevlere sahip olabilir. Expert sistemlerde birçok farklı temsil şekli vardır, ve en yaygını kural tabanlı (rule- base)olanıdır. Kural tabanlı sistemler, sistem trafiğini inceleyip kurallar oluşturur ve saldırı tespiti sırasında belirlenen kurallara göre davranışlar sınıflandırılır[17]. Fakat bir expert sistemin faydası, bilgi temsilinin şeklinden çok, temel olarak, sistemin bilgi tabanındaki bilginin kalitesine bağlıdır. Bu, kişiyi, gerçek uygulamalarda çok önemli olan bilgi edinme problemine yol açar. Bir expert sistem CD 'si örneği bir güvenlik planlaması içindir.[18] Bu expert sistemi, güvenlik derecesi seçimini önemli ölçüde kolaylaştırır, ve sınırlı kaynakların üst düzeyde

kullanımı için yol gösterir. Ve sınırlı kaynakların optimal kullanımı için rehberlik eder. Uzman sistemler kullanılarak saldırı erken tespit edilebilir.[19,20]

C. İntelligent Agents (Zeki Ajanlar)

Bilgisayar bilimlerin açısından zeki kelimesi, bir ajanın herhangi bir işlemi belirli inisiyatifler kullanarak yerine getirmesidir. Örneğin zeki olmayan bir vekil, her adımda ve her işlemde kullanıcıya bir şeyler sorarken, zeki vekilde daha çok otonom bir yapıdan (autonomous) bahsedilebilir[21]. Zeki ajanlar, onları özel kılan akıllı davranışları olan özelliklere sahip yazılım bileşenleri olmalarıdır. Bir ajan,ajan iletişim dilinin anlama (ACL) , reaktivitesi(bazı kararları alması ve hareket etmesi), planlama yeteneği, hareketlilik (mobility) ve yansıtma yeteneği gibi özelliklere sahiptir. Yazılım mühendisliğinde, yazılım ajanlarının en azından önleyici nesneler olduğu kabul edilir. Akıllı ajanlar kullanan savunma sistemleri tarif edilmiştir[22] ve simülasyonla işbirliği yapan ajanların DDoS saldırılarına karşı savunma gösterdiği görülür. Kısaca DDoS adı verilen saldırı türünden bahsedecek olursam, belirli bir siteye ya da sunucuya, yanıt veremeyeceği kadar sahte erişim isteği yollanır. Bunun sonucunda, site sunucunun taleplerini karşılayamaz hale getirerek kendini kapatır[24]. Zeki ajanlar DDoS a karşı savunma yapmaktadırlar.

Bazı yasal çözümlerden sonra ve aynı zamanda ticari sorunlardan, akıllı mobil ajanları oluşturan bir "siber polis" geliştirmek mümkün olmalıdır. Bu, siber ajanların hareketlilik ve iletişim altyapısının desteklenmesi için uygulanması gerekecektir. Fakat düşmanlar için erişilmez olmalıdır. Çoklu ajan araçları, siber uzayın tam operasyonel gözükmesini sağlayabilir, örneğin; melez bir çoklu ajan ve sinir ağı tabanlı saldırı tespit yöntemleri denenmiştir ve ajan tabanlı sistemler tarafından saldırlar tespit edilmiştir[25].

D. Genetik Algoritmalar

Genetik algoritmalar, karmaşık düzenli problemlerin çözümünü gerçekleştirmek amacıyla, kromozomların yeni diziler üretme esasını temel alan, sezgisel bir araştırma yöntemidir. Genetik algoritmaları diğer araştırma yöntemlerinden ayıran özellik ise, bir çözüm seti ile başladıktan sonra, geliştirme için biyolojik evrimi esas alan bir prosesin kullanılmasıdır. Bu prosesin sonunda en iyi kromozoma ulaşma amaçlanmaktadır.

Genetik algoritmalar siber savunmada, trafik verilerine basit kurallar uygulamak için kullanılabilir. Bu kurallar, anormal trafik verilerinden normal verileri ayırmak içindir. Veri kümesi, tcpdump ya da snort gibi trafik dinleyiciler (sniffers) kullanılarak toplanır [29]. Genetik algoritmalar öncelikle küçük boyutlu rastgele üretilmiş kurallar kümesi ile başlar, daha sonra bu kural kümesi genişletilir.

E. Fuzzy Logic (Bulanık Mantık)

Bulanık mantık tam ve kesin olmayan bilgilere dayanarak tutarlı ve doğru karar vermeyi sağlayan düşünme, karar verme, sonuç çıkarma mekanizmasıdır[30]. Boole mantığı yada programcılıktan gördüğümüz Boolean(true-folse, doğru-yanlış, var-yok)gibi kesin bir ifadesi olmayan 3 durumu da ifade eden bir yargıdır.Bulanık mantıkta "küçük","büyük","orta" gibi değerler alabilir.

Bulanık mantık metodunu uygulama girişimleri, CD'nin farklı bileşenlerinin geliştirilmesi için 2000'li yıllarda başlamıştır. Bu çalışmalarla ortaya çıkan FIRE (Fuzzy Intrusion Recognition Engine) ile AI verileri işlendikten sonra saldırıları tespit etmek için bulanık mantık kullanılmıştır [31]. AI paketleri üzerinde çalışılan FIRE'de, TCP, UDP ve ICMP için otonom ajanlar kullanılır [32]. Aynı zamanda kural tabanlı bir sistem olan bu çalışmada, güvenlik yöneticisi ve edinilen tecrübe sayesinde belirlenen bulanık kurallar oluşturulmuştur [33]. 2002 yılında bulanık mantığın, anormallik tespiti yapan bir CD'nin karar verme aşamasında kullanılması önerilmiştir [34]. Bu çalışmada bulanık mantık, uzman tarafından tavsiye edilen, bulanık "if-then" kurallarını temel alarak çözüm sunmaktadır.

F. Search (Arama)

Arama , evrensel bir yöntemdir. Tüm problem çözme durumlarında uygulanabilirken, diğer metotlar problem çözmede uygulanamayabilir. İnsanlar, buna dikkat etmeden sürekli olarak günlük yaşamlarında aramayı kullanırlar. Arama sorununun resmi ortamda bazı genel arama algoritmalarını bilmesi gerekir, bir çözüm yolu oluşturmak mümkün olmalıdır ve bir prosedür çözüm için önerilen yolun gerekli şartları yerine getirip getirmediğine karar vermek için kullanılabilir olması gerekir. Ancak, arama rehberi istismar edilirse, daha sonra arama verimliliğini önemli ölçüde değiştirebilir. Aramanın hemen hemen her akıllı programda bazı formu mevcuttur ve verimlilik genellikle tüm programın performansı için önemlidir.

Çok çeşitli arama yöntemleri geliştirilmiştir ki onlar belirli arama sorunları hakkında özel bilgi alır. AI'da bir çok arama yöntemi geliştirilmiş olmasına rağmen ve yaygın olarak bir çok programda kullanılan, nadiren AI kullanımı olarak kabul edilir. Örneğin; dinamik programlama aslında nadiren AI kullanımı olarak kabul edilen en iyi güvenlik sorunlarının çözümünde kullanılır, arama yazılım içinde gizlidir ve o bir AI uygulamasında görünmez değildir.

Ve veya arama ağaçlarında , alfa beta arama min max arama ve skolastik arama oyun yazılımında yaygın olarak kullanılanlardır ve onlar siber savunmada karar verme için yararlıdır. Alfa beta arama algoritmasında, aslında bilgisayar satranç için geliştirilmiş, problem çözmede" böl ve yönet" genel olarak yararlı bir fikir uygulamasıdır. Özellikle iki düşman ellerinden gelen eylemleri seçerken karar vermede kullanılır. Min tahminleri garanti kazanmak ve max mümkün kayıp tahminlerini kullanırlar. Bu seçenekler sayesinde sık sık büyük miktarda görmezden gelme ve oldukça hızlı aramalar yapmamızı sağlar.

G. Learning (Öğrenme)

Öğrenme, bilgi tabanını genişleterek veya yeniden organize ederek, ya da çıkarsama motorunu geliştirerek bir

bilgi sistemi geliştirmek demektir[35]. Bu yapay zekanın yoğun bir araştırma altında olan en ilginç problemlerinden biridir. Makine öğrenimi, yeni bilgi edinimi için, yeni beceriler ve var olan bilgiyi organize etmede kullanılan bilişim metotlarını içerir. Öğrenmenin problemleri, bazı parametrelerin öğrenme değerleri anlamına gelen parametrik öğrenmeden, öğrenme kavramı, dil bilgisi, işlevler, hatta davranış öğrenmeyi içine alan sembolik öğrenmenin karışık formlarına değişir. AI denetimli öğrenme(bir öğretmen ile) ve denetimsiz öğrenme gibi yöntemler sağlar. İkincisi verilerin yüksek miktarda bulunması durumunda özellikle faydalıdır ve CD de yaygındır çünkü CD de büyük günlükler bulunmaktadır. Veri madenciliği, gözetimsiz öğrenmenin gelişmesini sağlamıştır. Veri madenciliğine kısaca deyinecek olursak Veritabanındaki saklı olayları ortaya çıkarmak için yapılan bilgi açılımıdır. Paternleri ve veriler arasındaki ilişkileri bularak kural çıkarmak için kullanılır. Bu şekilde, hesap izlerini kullanarak normal kullanıcı aktiviteleri tanımlanır[37].

VI. ZEKİ SİBER SAVUNMA İÇERİSİNDEKİ ZORLUKLAR

Gelecekteki araştırma planlanırken, siber savunmadaki yapay zeka yöntemleri geliştirme ve uygulama, hedefler ve uzun vadeli perspektifleri ayırt etmek için olmuştur. Siber savunmaya hemen uygulanabilir birçok AI yöntemi uygulanabilmesine rağmen acil siber savunma problemleri vardır ki onlar şuanda kullanılan ve daha zeki çözüm gerektiren problemlerdir. Şimdiye kadar mevcut uygulamalardan bahsettim. Peki ya gelecekte? Gelecekte, bir durum yönetimi bilgi işlemenin tamamen yeni ilkelerinin uygulandığı umut verici ve karar veren perspektifler görebilirsiniz. Bu ilkeler modular bir tanıtımı içerir ve karar veren yazılım hiyerarşik bilgi mimarisini içerir. internet merkezli savaş için bilgi yönetimi zor bir uygulamadır[38]. Sadece otomatik bilgi yönetimi hızlı durum değerlendirmesi liderlerine bir karar üstünlük verdiğini garanti edebilir. Uzman sistemler halihazırda birçok uygulamada kullanılmaktadır. Bazen uygulamanın içinde saklı, yazılım planlama güvenlik önlemleri gibi. Ancak , uzman sistemlerden daha iyi performans alabilirsiniz, eğer geniş bilgi tabanları geliştirilirse. Bu bilgi edinme için büyük modül bilgi tabanlarının geliştirilmesi önemli miktarda yatırım gerektirecektir . Uzman sistem teknolojisinin daha da geliştirilmesi gerekecektir. Modülerlik uzman sistem araçlarında tanıtılmış olmalıdır ve hiyerarşik bilgi tabanlarını kullanılması gerekir.

Daha uzak bir gelecekte en azından önümüzdeki bazı yıllar belki de “narrow AI” bizi kısıtlayabilir. Bazı insanlar yapay zekanın büyük hedefleri olduğuna düşünmekteler. General yapay zekanın gelişimi[AGI] , AGI’ya bulunduğumuz yüzyılın ortasında ulaşılabilir. AGI ile ilgili ilk konferans 2008 yılında Memphis üniversitesinde yapıldı. Yapay zeka için Singularity enstitüsü[SIAI), 2000 yılında kuruldu, araştırmacılar bilgisayarlarda ki oluşabilecek zekanın katlanarak hızlı gelişimi konusunda uyarıyor. Bu gelişme Singularity’ e yol açabilir[39]’ de şöyle tarif ediliyor:” Singularity insandan daha akıllı zeka teknolojisinin yaratılmasıdır. Çeşitli teknolojiler vardır ki onların sık sık bu yönde ilerlediği sanılmaktadır. En sık bahsedilen muhtemelen yapay zeka olduğu fakat başkaları da var.—bi kaç farklı teknoloji ki onlar, onlar insan zekasından daha akıllı oluşturulmasını sağlayacak sofistike bir eşik seviyesine ulaşmıştır.” Singularity tehdidine inanmamak gerek fakat bilgi teknolojilerinin hızla gelişmesi önümüzdeki yıllarda yazılım içerisinde kesinlikle oldukça iyi bir zekanın inşasını sağlayacak(IBM’S WATSON programının son etkileyici performansını düşünün). Siber savunmanın suçluların ona sahip olduğundan daha iyi yapay zeka AI kullanma becerisine sahip olması çok önemlidir.

VII. DÜNYADA SİBER SALDIRI ÖRNEKLERİ

Soğuk Savaş sırasında Rusya ve ABD’nin karşılıklı casusluk faaliyetleri yaptığı biliniyordu. Moskova, 1982 yılında Kanada’da bir şirketten doğalgaz boru hatlarını kontrol etmek için kullanılan bir yazılımı çalmaya başladı. Bunu fark eden Amerikalılar ise, operasyonu durdurmak yerine yazılımın içine virüs yerleştirdiler. Rusların çaldığı yazılım bir süre sonra virüs tarafından bozuldu, boru hatlarındaki akışı anormal seviyelere çıkartı ve borunun patlamasına neden oldu. Sonuçta o güne kadar uzaydan görülen en büyük (nükleer olmayan) patlama yaşandı. Bu olay tarihe ilk siber saldırı olarak geçti.

ABD, 1992 yılında daha savaş başlamadan Irak devletinin tüm telekomünikasyon alt yapı şebekesini bir tuşla çökertmiştir. Oysa Saddam iletişim alt yapısını en son teknoloji ile yenilmek için çok büyük paralar harcamıştı. Hatta o yıllarda dünyadaki en son teknolojik gelişmelerin uygulandığı sayısal haberleşme sistemleri Irak’ta kurulmuştu. Tüm askeri birliklerin birbirleri ile olan iletişimi bir tuşla çökertilmiştir. Hem de çok uzaklardan, bir tuşa basılarak uzaydaki uydu üzerinden bir komut gönderildi ve tüm iletişim sistemlerinin çalışması aynı anda bloke edildi. 2003 yılında ABD Irak'ı işgal etmeyi planlarken Irak Savunma Bakanlığı’nda çalışan binlerce kişi, işgalden hemen önce bilgisayar ekranlarında Amerikan Merkez Komutanlığı’ndan gelen bir mesaj gördüler. Mesajda, “Yakın bir zamanda Irak’ı işgal edebiliriz. Sizlere zarar vermek istemiyoruz. Başınıza bir şey gelmesini istemiyorsanız savaş başladığında evlerinize gidin” diyordu. Birçok kişi hatta askerler bu mesajı ciddiye alıp tankları terk edip evlerine gitti. ABD böylece Irak tanklarını kolaylıkla imha edebildi.

Siber saldırı ve savunma sistemlerinde en güçlü olduğu tahmin edilen ülkelerden biri olan Çin’in, ABD’nin askeri ve Avrupa’nın teknoloji sırlarını elde etmeye çalıştığı iddia edilmektedir. Amerikan askeri araç ve silahlarının üreticisi Lockheed Martin’in gizli bilgilerine eriştiği iddia edilen Çin’in siber istihbarat uzmanlarının, F-35 savaş jetlerinin tüm planlarını ele geçirdikleri iddia edilmektedir.

İsrail uçakları, 6 Eylül 2007’de, Türkiye’nin Suriye sınırından 120km içerde bir inşaatı bombaladı. Bir nükleer

tesis olduğu zannedilen bina bir gece içinde yerle bir edildi. Suriye'nin ancak sabah haberi oldu. Oysa Rusya'dan satın aldıkları güçlü radarların İsrail uçaklarının hava sahasına girişini görüntülemiş olması gerekirdi. Soruşturmanın ardından İsrail'in Suriye savunma ağına yerleştirdiği bir yazılım radarlardaki görüntüyü her şey normal olarak izlettirdi. Yani İsrail uçaklarının ülke sınırları içinde olduğu anlarda Suriyeli askeri yetkililer tertemiz bir radar görüntüsü izliyorlardı ve dolayısıyla olaysız bir gece yaşadıklarını zannediyorlardı. İsrail bu siber saldırıyı yapmak için; saldırıdan önce Suriye hava savunma sahasına gizlice sokulan insansız hava araçları bozuk sinyal göndererek radarlarda arıza ve karışıklık oluşturdu. Bu sırada İsrail tarafından Suriye hava sahasını denetleyen bilgisayar koduna tuzak kapan yazılımı yerleştirildi. Ağ sisteminin kontrolünü ele geçirmek için kullanılan bu kapan yazılımı radardaki görüntüyü İsrail'in istediği gibi değiştirdi. İsrailli bir ajan, Suriye sınırları içinde internet bağlantısı sağlayan fiber ağ teknolojine izinsiz erişim yaparak radardaki görüntü kontrolünün İsrail'e geçmesini sağladı.[1]

"... Siber saldırıda, Estonya Cumhurbaşkanlığı, parlamento, birçok bakanlık siyasi partiler ve bankalarla diğer işletmelerin internet sitelerinin hedef alındığı, aşırı yüklenme nedeniyle ana işlemcilerin çöktüğü ve ülkenin dış dünyayla bağlantısının kesilme noktasına geldiği belirtiliyor." (17 Mayıs, 2007, BBC)[41]

En büyük sistem olan ve 'Global bir network sistemi' olarak tanımlanan ECHELON dünyadaki iletişim trafiğinin çoğunu eş zamanlı olarak izleyebilmektedir (elektronik posta, telefon, fax, telex, telgraf, kablo vs). Dünyada internet üzerinden yapılan tüm yazışmalar, e-mail'ler Amerika'da Echelon sistemi içinde yer alan 'root server' denilen 13 tane kök bilgisayardan geçiyor. Echelon dakikada 8 milyon, günde ise tam 12 milyar telefon görüşmesini izliyor ve dinliyor.ECHELON'dan farkı ise, izlediği kişi, grup, nesne yada objeler hakkında yapay zeka aktivasyonları ile tüm internet omurgalarına (backbone) kendiliğinden bağlanarak, içerdiği anahtar kelimeler ile ilgili tüm sistemlere hacker gibi girerek avcılık yapmasıyla ünlüdür[41].

VIII. SİBER SALDIRI İÇİN ALINAN ÖNLEMLER

Dünyada birçok ülkenin siber saldırı ve savunma sistemlerine özel bütçe ayırdığı ve yoğun çalışmalar yaptıkları bilinmektedir; ABD de gizli bilgilerin bulunduğu ağ sistemlerine girme amaçlı yapılan birkaç ciddi saldırıdan sonra Pentagon ve Ulusal Güvenlik Servisi'nin işbirliği ile siber savaş ve siber istihbarat birimi kurulmuştur. Siber savunma uzmanlarını işe almaya ve eğitmeye başladılar. İsrail askeri istihbarat örgütüne bağlı elektronik istihbarat ünitesi, siber saldırı güvenliğini sağlamak amacıyla özel birim kurmuştur. Sanal aleme bağlı olarak işleyen otomasyon sistemlerinin ve finansal kurumların güvenliğini sağlamakla görevlendirilen bu birim, halen ulusal istihbarata bağlı çalışmaktadır. Çin, siber savaş gücünde ABD'den sonra en güçlü ülke olarak görülmektedir. Rusya'da internet ortamından saldırı konusunda uzmanlaşmış çok sayıda profesyonel mühendisin olduğu bilinmektedir. İllegal olarak yazılım geliştirip internet ortamında satan bu mühendisler dünyadaki çok sayıdaki şirketleri mağdur etmişlerdir. İngiltere de Siber Savunma Operasyonları Merkezi adlı birimde İngiliz istihbaratına bağlı binlerce siber casus görev yapmaktadır. İngiltere hükümeti istihbarat bilgilerinin siber saldırılar sonucu dışarı sızmasını engellemek amacıyla bir ekip oluşturmuştur. Kuzey Kore'nin siber saldırı ve savunma gücünü geliştirmek için çoğu askeri akademiden mezun yüzlerce siber korsandan oluşan bir ekip oluşturduğu bilinmektedir. İran'ın siber saldırı ve savunma ordusuna sahip olduğu iddia edilmektedir[1].

Japon Savunma Bakanlığı'nın 2008'den beri Fujitsu ile ortak çalışmalar yürüttüğü ve savunma amacıyla kullanılacak, saldırgan bir bilgisayar virüsü hazırladığı ortaya çıktı.Savunma virüsü siber saldırılar anında, saldırının geldiği tüm kaynakların izini sürerek hepsini tek tek kapatmaya yarıyor. Aslına bakarsanız teoride bu virüsün internete bağlı olan tüm PC ya da sunuculara saldırarak etkisiz hale getirmesi de mümkün demek oluyor.Tabii bu en büyük felaket senaryosu ve diğer ülkelerin de bu tarz virüsler üzerinde çalıştıkları ya da en azından çalışmaya başlayacakları da bir gerçek[42].

IX. SONUÇ VE DEĞERLENDİRME

Bu çalışmada, siber savunmada yapay zeka teknikleri genel olarak incelenmiş, gözden geçirilmiştir. Son zamanlarda oluşan siber saldırılardan dolayı siber savunma isteği daha çok artmıştır. Siber savunma yazılımlarının görevini yerine getirebilmesi için basit algoritmaların yeterli olmadığı, yapay zeka algoritmalarının kullanılmasının daha uygun olduğu sonucu çıkmaktadır. Yapılan araştırmalar sonucunda siber savunmada yapay sinir ağlarının daha fazla kullanıldığı görülmüştür. Tabi elimizde olan yapay zeka teknikleri bir kısım siber savunma yöntemlerini karşılamamaktadır. Karşılanamayan noktalar; karar destek, durum farkındalığı ve bilgi yönetimidir. Bun noktaların karşılanabilmesi için uzman sistem teknolojisinde çalışmalar devam etmekte ve çalışmaların olumlu sonuçlanacağı düşünülmektedir.

Son olarak General yapay zekaya değinecek olursam yüzyılın ortalarına doğru tam anlamıyla gelişmesi beklenmesine rağmen nasıl hızlı bir gelişme gösterip önde gittiği görülmektedir. Fakat generel yapay zekanın siber savunmada kullanılacağı gibi saldırganlar tarafından en kısa sürede kullanılacağı düşünülmektedir.

KAYNAKLAR

[1] ylt44.com/bilimsel/siber.pdf

[2] Ş. Sağıroğlu, M, Alkan, "Her yönüyle elektronik imza (e-imza)",Grafiker Yayınları, Ankara, 1-100 (2005).

[3] Sundaram, "An introduction to intrusion detection", Crossroads: The ACM Student Magazine, New York, USA, 2(4), 3-7 (1996).

[4] http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/tahir_emre_kalayci_tez.pdf

[5] http://en.wikipedia.org/wiki/Conficker

[6] R. E. Wassmer, J. H. Fikus, "Advanced Intrusion Detection Techniques", Final rept., Defense Technical Information Center - ADA410454, 2. evre, 1-14, (2003).

[7] J. Cannady, "Artificial neural networks for misuse detection", Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, 443-456 (1998).

[8] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85-460-1, Cornell Aeronautical Laboratory, 1957.

[9] Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. Military Communications and Information Systems Conference (MCC), Wroclaw, Poland, 2010.

[10] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," in SIN '09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229–234.

[11] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection," in International Joint Conference on Neural Networks (IJCNN), 2006, pp. 2362–2369.

[12] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, vol. 36, no. 3, Part 1, 2009, pp. 4321–4330.

[13] P. Salvador et al. Framework for Zombie Detection Using Neural Networks. In: Fourth International Conference on Internet Monitoring and Protection ICIMP-09, 2009.

[14] M. Shankarapani, K. Kancherla, S. Ramammoorthy, R. Movva, and S. Mukkamala. Kernel Machines, for Malware Classification and Similarity Analysis. WCCI 2010 IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010, pp. 2504 – 2509.

[15] B. Fei, J. Eloff, MS Olivier, H. Venter. The use of self-organizing maps of anomalous behavior detection in a digital investigation. Forensic Science International, v. 162, 2006,pp. 33-37.

[16] http://en.wikipedia.org/wiki/Expert_system. Expert System. Wikipedia.

[17] K. Ilgun, R. Kemmerer, P. Porras, "State Transition Analysis: A RuleBased Intrusion Detection System", Software Engineering, 21(3):181-199 (1995).

[18] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.

[19] D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES). Technical Report SRI-CSL-95-07, SRI International, Computer Science Lab (1995).

[20] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System. Proc. IEEE Symposium on Security and Privacy, 1988, p. 59.

[21] http://www.bilgisayarkavramlari.com/2010/02/15/zeki-vekiller-akilli-ajanlar-intelligent-agents-zeki-etmenler/

[22] Kotenko, A. Ulanov. Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks. In: International Workshop on Autonomous Intelligent Systems: Agents and Data Mining. LNCS, Springer, v. 4476.

[23] Kotenko, A. Konovalov, A.Shorov. Agent-Based modeling and Simulation of Botnets and Botnet Defence. In: C. Czosseck, K. Podins (eds.). Proc. Conference on Cyber Conflict. CCD COE Publications, Tallinn, Estonia, 2010.

[24] http://systemcontrol.blogcu.com/siber-savas-da-nedir/9087496

[25] V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A Distributed Intrusion Detection Prototype Using Security Agents. HP OpenView University Association, 2004.

[26] B. Stahl, D. Elizondo, M. Carroll-Mayer, Y. Zheng, K. Wakunuma. Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics. In: WCCI 2010 IEEE World Congress on Computational Intelligence, Barcelona, Spain. 2010, pp. 1822 – 1829.

[27] E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid multi agent-neural network intrusion detection with mobile visualization," Innovations in Hybrid Intelligent Systems, vol. 44, 2007, pp.320–328.

[28] http://www.necdetozcakar.com/wp-content/uploads/Genetik-Algoritmalar.pdf

[29] Murali, M. Rao, "A survey on intrusion detection approaches", First International Conference on Information and Communication Technologies, IEEE Communications Society Press, 233-240 (2005).

[30] http://www.suatustkan.com/userfiles/Makalelerim/yapay_zeka.pdf

[31] J. E. Dickerson, J. A. Dickerson, "Fuzzy network profiling for intrusion detection" NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, 301-306, (2000).

[32] J. E. Dickerson, J. Juslin, O. Koukousoula, J. A. Dickerson, "Fuzzy intrusion detection", IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference, Vancouver, British Columbia, 3: 1506-1510 (2001).

[33] K. Lee, L. Mikhailov, "Intelligent Intrusion Detection System", Second IEEE International. Conference on Intelligent Systems, 2: 497-502 (2004).

[34] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection System", IEEE Transactions on Systems, Man, and Cybernetics, Part C 32(2): 154-160 (2002).

[35] P. Norvig, S. Russell. Artificial Intelligence: Modern Approach. Prentice Hall, 2000.

[36] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on Learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.

[37] W. Lee, S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, S. Hershkop, J. Zhang, "Real time data mining-based intrusion detection", Second {DARPA} Information Survivability Conference and Exposition (DISCEX II), Anaheim, CA, 89-100 (2001).

[38] J. Kaster. Combined Knowledge Management and Workflow Management in C2 Systems – a user centered approach. Fraunhofer Institute for Communication, Information Processing and Ergonomics. Report ID # 197, 2009.

[39] http://singinst.org/overview/whatisthesingularity/

[40] http://www.ted.com/webcast/archive/event/ibmwatson

[41] http://www.sosyalistforum.net/bilisim-guncel-haberler/31307-iletisimde-bilgi-guvenligi-ve-siber-savaslar.html

[42] http://shiftdelete.net/japon-hukumeti-savunma-virusu-hazirliyor-34106.html

[43] http://systemcontrol.blogcu.com/siber-savas-da-nedir/9087496

[44] http://www.hakikat.com/dergi/208/ukara208.html

[45] E. Tyugu, R&D Branch, "Artifical Intelligence in Cyber Defence", IEEE Xplore