YAPAY ZEKA TEKNİKLERİNİN / UYGULAMALARININ SİBER SAVUNMADA KULLANIMI

Ensar Şeker

NATO CCD COE
Tallinn, Estonya
ensar.seker@ccdcoe.org

ÖZET

Günümüzde siber savunma alanındaki süreçlerin hızı ve kullanılan veri miktarının çokluğu dikkate alındığında, otomasyon sistemlerinin yardımı olmaksızın, salt insan gücü kullanılarak etkili bir savunma meydana getirilmesi beklenemez. Bununla birlikte, ağlardaki dinamik olarak gelişen saldırılara karşı, etkin bir savunma için, klasik sabit algoritmalar ile yazılım geliştirmek zordur. Bu durumun üstesinden, yazılım için esneklik ve öğrenme kabiliyeti sağlayan yapay zeka yöntemleri kullanılarak gelinebilir. Savunma sistemlerinin zekasının arttırılması yoluyla siber savunma yeteneklerinin geliştirilmesi ihtimali oldukça yüksektir. Gerçek hayatta siber savunma ile ilgili sorunlara bakıldığında birçok siber savunma probleminin ancak yapay zeka yöntemleri kullanıldığında başarıyla çözülebileceği açıkça görülmektedir. Bu makalede mevcut yapay zeka uygulama ve teknikleri gözden geçirilerek, yapay zekanın siber savunma sistemlerinde kullanımı ve bu kullanımın zorunluluğu ve öneminden bahsedilmiştir. Makalenin amacı, hali hazırda geliştirilmekte olan yapay zeka teknoloji ve metodolojilerini ele alıp inceleyerek, bu teknoloji ve metodojilerin siber savunmadaki rolü ve adaptasyonu konusuyla entegre ederek, bahsi geçen bu yöntemlerin siber savunma alanında kullanımını güncel örneklerle açıklayabilmektir.

***Anahtar Kelimeler*—**Yapay zeka, siber savunma, erken uyarı sistemleri, saldırı tespit ve önleme sistemleri.

Use of Artificial Intelligence Techniques / Applications in Cyber Defense

ABSTRACT

Nowadays, considering the speed of the processes and the amount of data used in cyber defense, it cannot be expected to have an effective defense by using only human power without the help of automation systems. However, for the effective defense against dynamically evolving attacks on networks, it is difficult to develop software with conventional fixed algorithms. This can be achieved by using artificial intelligence methods that provide flexibility and learning capability. The likelihood of developing cyber defense capabilities through increased intelligence of defense systems is quite high. Given the problems associated with cyber defense in real life, it is clear that many cyber defense problems can be successfully solved only when artificial intelligence methods are used. In this article, the current artificial intelligence practices and techniques are reviewed and the use and importance of artificial intelligence in cyber defense systems is mentioned. The aim of this article is to be able to explain the use of these methods in the field of cyber defense with current examples by considering and analyzing the artificial intelligence technologies and methodologies that are currently being developed and integrating them with the role and adaptation of the technology and methodology in the defense of cyberspace.

Keywords— Artificial intelligence, cyber defense, early warning systems, intrusion detection and prevention systems.

I. GİRİŞ (INTRODUCTION)

Günümüzde siber alan tüm verileri ile birlikte zettabayt çağına erişmiştir. Yeni teknolojilerin ve hizmetlerin yanı sıra trilyonlarca aygıt ve zettabayt verinin ortaya çıkması, eski tehditlerin ve güvenlik açıklarının ele alınmasının yanı sıra siber güvenlik uzmanlarını yeni tehdit ve zayıf noktalarla da uğraşmak zorunda bırakmıştır. Buna ek olarak siber savaş alanındaki teknolojik gelişme ve ilerlemeler ile karmaşık tehditler, siber savunmada daha akılcıl çözümlere baş vurulma gerekliliğini meydana getirmiştir.

Yeni teknolojilerin siber savunma sistemlerine adapte edilmesi, bu sistemleri hedef alabilecek tehditlerdeki teknolojik artış göz önünde bulundurulduğunda ne derecede kritik olduğu ortaya çıkmaktadır. Yeni teknolojiler arasında yapay zekaya siber savunmada daha ağırlık verilmesi siber saldırıların daha erken tepit edilmesi ve bu saldırılara daha erken karşılık verilmesine katkı sağlamaktadır.

Siber savunma alanıında yapay zeka kullanımı ile ilgili ele alınması gereken temel problem mevcut teknolojilerin arzu edilen yeterli seviyede olmadığı ve siber savunmanın en zayıf haklası olarak kabul edilen insan faktörünün en aza indirgene bilmesi için ne gibi yapay zeka metodojilerinin geliştirilerek adapte edilmesi gerektiği konusundadır.

Bu çalışmada öncelikle yapay zeka konusu ele alınmış, bu kavramdan ne kastedildiği, ayrımları, bu teknolojiyi geliştirmekteki zorluklardan bahsedilmiştir. Daha sonraki bölümlerde ise makalenin ana konusunu teşkil eden geliştirilmekte olan yapay zeka teknik ve yöntemlerinin siber savunma sistemlerinde nasıl kullanıldığı konusu açıklanmaya çalışılmıştır. Özellikle erken uyarı, saldırı tespit ve önleme sistemlerinde yapay zeka kullanımı oldukça önemlidir. Yine siber savunma için kullanılan mevcut yapay zeka uygulamalarını incelemek, gittikçe daha büyük önem kazanan bu konuyla ilgili gelecekte yapılması düşünülen bilimsel çalışmalara da katkı sağlayabilecektir.

II. YAPAY ZEKA

Yapay zeka, akıllıca davranabilen ve normal olarak insanlar tarafından yapılabilecek görevlerin - eşit derecede - veya bazen daha iyi - yetenekli olan sistemlerin ve yazılımların geliştirilmesiyle uğraşan bir bilgisayar bilimi alt dalıdır. Geliştirilen birçok bilişsel yapay zeka yöntemi (patern tanıma, bilişsel zeka, sinir ağları, akıllı ajanlar, yapay bağışıklık sistemleri, makine öğrenimi, veri madenciliği, bulanık mantık, buluşsal yöntemler, vb.) siber alanda aktif bir şekilde kullanılmaktadır [1].

Salt düşünme yeteğinin yanında bir insanın nasıl düşüneceğini temel alarak sonuçlar üretmeye dayanan yapay zeka, güçlü yapay zeka olarak adlandırılırken bir insan gibi hareketler sergiliyebilmesine rağmen bir insan gibi düşünemeyen yapay zeka, zayıf yapay zeka olarak adlandırılmaktadır [1]. Bu ayrım bazı kaynaklarda (düşünme/davranma, insanca/mantıksal) olarak da yapılabilmektedir [13]. Bir insan gibi düşünen ve çıktılarını bir insanın nasıl düşündüğü sorusu üzerine temellendiren gerçek simülasyonların (güçlü yapay zeka) veya sistemlerin, gerçek bir modeli bilindiği kadarıyla henüz mevcut değildir. Bu nedenledir ki olayları bir insan gibi algılayıp, tepkiler veren bir yapay zeka meydana getirmenin çözülmesi çok zor bir problem olduğu bilinmektedir. Zayıf yapay zekaya verilebilecek en iyi örnek IBM tarafından satranç oyunu için geliştirilen Deep Blue adlı bilgisayardır. İyi bir satranç oyuncusu olmasına karşın Deep Blue bir insan gibi düşünerek hamlelerini yapamamaktadır. Bu iki kategorinin dışında üçüncü bir kategori olarak zayıf ve güçlü arasında geliştirilen yapay zeka örnekleri de mevcuttur. Bu sistemler bir insan gibi akıl yürütmeyi bir kılavuz olarak kullanabilmekle birlikte mükemmel bir modelleme hedefi ile yönlendirilememektedirler. Bu tür bir sisteme verilebilecek en iyi örneklerden bir tanesi yine IBM tarafından geliştirilen IBM Watson'dır. Watson doğal dilde hazırlanmış sorulara cevap verme kapasitesine sahip bir soru-cevap bilgisayar sistemidir. Metindeki kalıpları tanıma yeteneğini, bu kalıplarla eşleşen kanıtları temel alarak birleştirme yetisine sahiptir [2, 3]. Konuyla alakalı bir başka örnek olarak Google tarafından geliştirilen Google Brain verilebilir. Google Brain, derin öğrenime dayalı bir yapay zeka araştırma projesidir. Google Brain in çalışma yapısı, beynin gerçek yapısından esinlenildiği için beyine benzer bir çalışma yapısına sahiptir. Nöronların davranışlarını temel alan derin öğrenme sistemleri, resim ve konuşma tanıma gibi görevler için öğrenme katmanlarıyla işlev görür [4].

Yapay zekalar için bir diğer ayrım genel yapay zeka ve dar yapay zekadır. Genel bir amaç için tasarlanan, çok özel bir amacı olmayan yapay zekalar genel yapay zeka olarak adlandırılırken, özel bir amacı gerçekleştirmek amacıyla tasarlanan yapay zekalar içinse dar yapay zeka terimi kullanılmaktadır [13].

III. SİBER SAVUNMADA YAPAY ZEKA

Siber savunma, kritik alt yapılara, kurum ve kuruluşların bilgi güvenliğine, hükümet ve Devlet birimlerine, bunlarla birlikte ulusal güvenlik kapsamında değerlendirilen diğer tüm ağlara karşı muhtemel siber saldırı ve tehditleri elemine etmek yada bu tehdit ve bunların doğurabileceği hasar ve zararları en aza indirgemek için geliştirilen bigisayar-ağ savunma mekanizmalarıdır. Siber savunma, saldırılara ve/veya tehditleri zamanında tespit ve engellemeyi sağlayıp, böylece altyapı ve/veya verilerin değiştirilmemesine odaklanmaktadır. Siber saldırıların hacminin yanı sıra karmaşıklığıyla birlikte, siber savunma çoğu kurum ve kuruluş için, hassas bilgilerin, verilerin ve varlıkların korunmasını sağlayabilmek adına şarttır. Siber savunma, saldırganlara karşı hassas

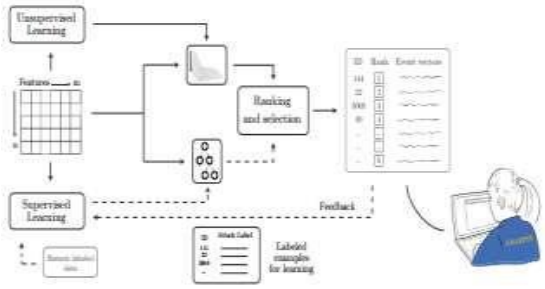
dereceli veri ve varlıkların bulunduğu ortamın cazibesini düşürme, kritik lokasyonları ve bilgiyi değerlendirme ve anlama, saldırı tespit ve reaksiyon ve karşılık verebilme kapasitelerini artırma ve saldırganların saldırabileceği yol, yöntem ve alanları teknik analizlerle tanıma gibi konuları da kapsamaktadır. Siber savunmanın, siber güvenlik katkılarının yanı sıra, güvenlik stratejileri geliştirme, kaynakları en etkin biçimde kullanma ve özellikle kritik noktalardaki güvenlikle ilgili kaynak ve giderlerinin etkinliğini artırmada da katkıları bulunmaktadır.

Bahsedildiği üzere siber saldırıların engellenmesi ve siber tehditlerden kaçınma siber savunmanın temel taşıdır. Bununla birlikte bu saldırı ve tehditleri tamamen elimine etmek mümkün değildir. Bu saldırı ve tehditlere karşı en hızlı karşılığı vermek ve olabilecek zararları en aza indirmek kritik derecede önemlidir. Mevcut güvenlik yazılım veritabanları ve algoritmaları sınırlı bir kapasiteye ve kabiliyete sahip olup çoğu zaman yeni tehdit vektörlerinin hızlı gelişimi ve değişimi ile başa çıkamamaktadır. Akıllı bir güvenlik sisteminde tasarlanmış yapay zeka algoritmaları, meydana gelen ve hatta değişen tehditleri tanımlama ve bunlara yanıt verme potansiyeline sahiptir.

Günümüzde, bilgi güvenliği çözümleri genellikle iki kategoriye ayrılır: analist yönlendirmeli veya denetlenmeyen makine öğrenme odaklıdır. Nadir veya anormal kalıpları tespit etmek için denetimsiz makine öğrenimini kullanmak, yeni saldırıların tespitini artırabilir. Bununla birlikte, daha fazla yanlış pozitif ve uyarıları da tetikleyebilir. Bu durum, bu yanlış pozitiflerin doğruluğunu araştırmak için önce önemli miktarda analiz çabası gerektirir. Bu tür hatalı alarmlar, alarm yorgunluğuna ve güvensizliğine neden olabilir ve zamanla, analitik odaklı çözümlere dönmesine ve buna bağlı zayıf yönlerin doğmasına neden olabilir. Bilgi güvenliği endüstrisinin karşı karşıya olduğu, her biri makine öğrenme çözümleri tarafından ele alınabilecek üç önemli zorluk şöyle belirlenmiştir [5]:

- Etiketli verilerin eksikliği yada olmaması: Birçok organizasyon, daha önce yapılmış saldırıların etiketli örneklerden ve denetlenen öğrenme modellerini kullanma kabiliyetinden yoksundur.
- Sürekli gelişen saldırılar: Denetimli öğrenme modelleri mümkün olsa da, saldırganlar davranışlarını sürekli değiştirerek söz konusu modelleri geçersiz kılabilmektedir.
- Araştırma yada Tetkik için Sınırlı Zaman ve Bütçe: Analistlere saldırıları araştırmak için başvurmak maliyetli ve zaman alan bir işlemdir.

Karşılaşılan bu güçlükleri giderebilecek çözümler, analistlerin zamanını etkili bir şekilde kullanmasına katkı sağlamalı, yeni ve gelişen saldırıları erken aşamalarında tespit etmeli, saldırıları algılama ile saldırı önleme arasındaki reaksiyon sürelerini azaltmalı ve son derece düşük yanlış pozitif orana sahip olmalıdır. MIT tarafından geliştirilen ve Yapay Zekaya dayanan ve AI2 olarak adlandırılan siber güvenlik platformu bu çözümleri sağlayabilmektedir [5].



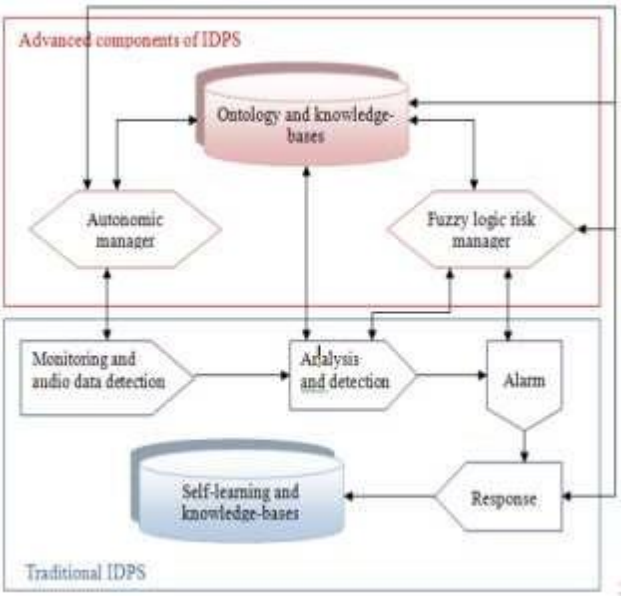
Şekil 1. AI2 [5]

A. Siber Savunmada Erken Uyarı, Saldırı Tespit ve Önleme Sistemleri

Muhtemel siber savunma sistemi en az üç düzeyde siber güvenlik sağlamalıdır. Birinci seviye, kimlik ve kimlik doğrulama, kriptografik koruma, erişim kontrolü, denetim, ağ filtreleme vb. gibi geleneksel statik siber savunma mekanizmaları içerir. İkinci seviye, bilgi toplama, güvenlik değerlendirmesi, ağ durumu izleme, saldırı gibi proaktif siber savunma mekanizmalarını içerir. Üçüncü seviye, ağ durumunun bütüncül değerlendirmesini, uygun veya optimal savunma mekanizmalarının seçimini ve bunların adaptasyonunu yerine getiren siber savunma yönetimine karşılık gelir [6].

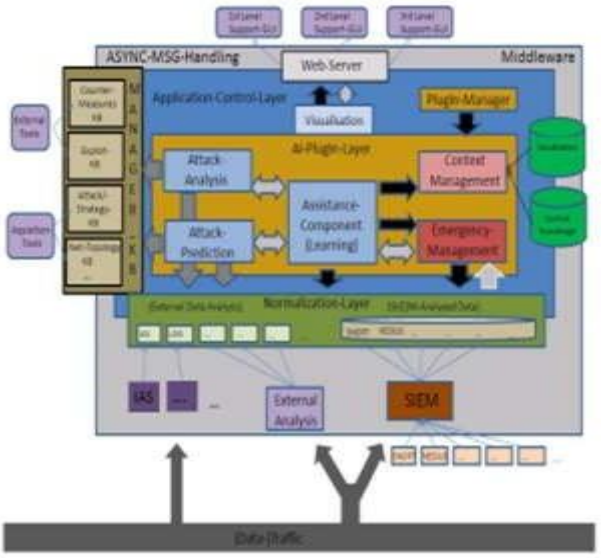
Söz konusu siber güvenlik düzeylerinin sağlanmasında içinde, yapay zeka teknolojilerini de barındıran erken uyarı, saldırı tespit, ve önleme sistemleri önemli rol oynamaktadır.

Siber saldırılara karşı koruma ve mümkün olan en kısa zamanda karşılık vermek için Erken Uyarı Sistemleri (EUS) kullanılmaktadır. Bununla birlikte yeni teknolojilerle gelişen yeni siber tehdit düzeyinden ötürü, geleneksel ve salt paket denetimine dayanan EUS den farklı olarak verileri toplayıp, analiz edip, ilişkilendirebilen ve aynı zamanda tehdit modellerini neredeyse gerçek zamanlı olarak algılayıp, analiz edip ve bunlara karşılık verebilen yeni EUS mimarisine ihtiyaç duyulmaktadır. Bu ihtiyaç, sanal sensörlerin geliştirilmesi, verilerin sofistike korelasyonu, ağ davranış analizi için yeni mantık modelleri, öğrenme algoritmaları ve özellikle IPv6 ağlarındaki ölçeklenebilirlik, güvenilirlik ve esneklikleri sağlayabilecek konseptleri ve yeni yaklaşımların geliştirilmesini içermektedir [7].



Şekil 2. Tipik bir Saldırı Tespit ve Önleme Sistemi [8]

Erken uyarı ve saldırı tespitlerinde Yapay Zeka kullanımında amaç hem yerel alan ağlarında hem de geniş alan ağlarında internetten gelen saldırıların olabildiğince erken tespit edilmesine yönelik gelişmiş, akıllı bir yardım sisteminin geliştirilmesidir. Bu çerçeve içinde, FTP, SMTP ve HTTP gibi yaygın olarak kullanılan internet protokolleri de düşünülmeli, aynı zamanda SOAP gibi daha yeni protokoller de dikkate alınmalıdır. Bu konuda geliştirilen projelerden bir tanesi FIDeS projesidir. FIDeS projesi sadece saldırı tespiti yerine, daha fazla yardıma (bir saldırı durumunda somut talimatlar gibi) odaklanmaktadır. Bu amaçla, bildirimsel bilgi temsili, açıklamalar üretilmesi ve bilişsel yardım gibi çeşitli Yapay Zeka tabanlı yöntemler kullanılır. Sistem güvenlik uzmanını saldırıları analiz etme ve karşı atak geliştirme konusunda desteklemek üzere tasarlanmıştır [9].



Şekil 3. FIDeS Sistem Mimarisi [9]

Ciddi siber saldırılar karşısında etkin bir siber savunma için saldırı tespit ve önleme sisteminin belli özelliklere sahip olması beklenmektedir. Bu özelliklerden bazıları şunlardır[10];

- Siber saldırı devam ederken veya hemen sonrasında gerçek zamanlı saldırı tespiti yapabilmek,
- Yanlış pozitif alarmları minimize etmek,
- İnsan gözetimini minimuma indirip ve operasyonların sürekliliğini sağlamak,
- Kazara olan veya saldırılardan kaynaklanan, sistemde meydana gelebilecek kayıplara karşı sistemin kurtarılabilirliği temin etmek,
- Saldırganların sistemde değişiklikler yapma girişimlerinin tespiti için, kendini denetleme yeteneğine sahip olmak,
- İzlenen sistemin güvenlik politikalarına uymak ve
- Zaman içindeki sistem değişikliklerine ve kullanıcı davranışlarına uyumluluk sağlamak,

B. Siber Savunma için Yapay Zeka Uygulamaları

Geleneksel sabit algoritmalar (hard-wired logic on decision making level) dinamik olarak gelişen siber saldırılarla mücadele etmek için etkisiz kalmaktadır. Bu nedenle, özellikle siber savunmada esneklik ve öğrenme kabiliyeti sağlayan yapay zeka yöntemlerini ve uygulamalarını kullanmak gibi daha yenilikçi yaklaşımlara ihtiyaç duyulmaktadır [11, 12].

Zekanın simüle edilebilmesi konusundaki genel problem, akıllı bir sistemin sergilemesi gereken belirli özelliklere veya yeteneklere sahip olan alt problemler belirlenerek basitleştirilmiştir. Bu alt problemlerden bazıları şöyledir; [13, 14]:

I. Çıkarım, mantık, problem çözme (gömülü ajanlar, sinir ağları, yapay zekaya istatistiksel yaklaşımlar);
II. Bilgi sunumu (ontolojiler);
III. Planlama (çoklu ajan planlaması ve işbirliği);
IV. Öğrenme (makine öğrenimi);
V. Doğal Dil İşleme (bilgi edinme - metin incelemesi, makina çevirisi);
VI. Hareket ve Manipülasyon (navigasyon, lokalizasyon, haritalama, hareket planlama);
VII. Algılama (konuşma tanıma, yüz, tanıma, nesne tanıma);
VIII. Sosyal Zeka (empati simülasyonu);
IX. Yaratıcılık (yapay sezgi, suni hayal gücü); ve
X. Genel Zeka (Güçlü yapay zeka).

Siber savunma göz önünde bulundurularak mevcut Yapay Zeka method ve mimarileri şu kategorilere ayrılabilir;

1) Sinir Ağları (Neural Nets): Sinir ağları, 1957'de Frank Rosenblatt tarafından "perceptron"un keşfi ile başlayan uzun bir geçmişe sahiptir. Makine öğreniminde perceptron, ikili (binary) sınıflandırıcıların (vektör numaraları tarafından temsil edilen girdinin belirli bir sınıfa ait olup olmadığına karar veren fonksiyonlar) denetimsel öğrenimi için geliştirilmiş bir algoritmadır. Bu sinir ağlarının en popüler elementlerinden biri yapay nörondur [15, 16]. Birlikte çalışan az sayıdaki perceptronlar sorunları öğrenebilir ve çözebilirler. Fakat sinirsel ağlar, çok sayıda yapay nörondan oluşabilir. Çok sayıda yapay nörondan oluşan sinir ağları, kitlesel paralel öğrenme ve karar verme işlevselliği sağlayabilmektedir. Bu ağların en belirgin özelliği operasyonel hızlarıdır. Pattern tanıma, öğrenme, sınıflandırma, saldırılara karşılık verme konuları için oldukça uygundurlar. Hem donanıma hem de yazılıma uygulanabilirler [17].

Sinir ağları, saldırı tespiti ve önleme için de uygundur [18, 19, 20, 21]. Söz konusu ağların DoS algılama [22], bilgisayar solucanı algılama [23], spam algılama [24], zombi algılama [25], kötü amaçlı yazılım sınıflaması [26] ve adli araştırmalar [27] içinde kullanmak yönünde bilimsel çalışma ve öneriler yapılmıştır.

Sinir ağlarının siber savunmada popüler olmasının bir nedeni, donanım içinde uygulanabilmesi ve grafik işlemcilerde kullanılması durumunda yüksek hızlarıdır. Üçüncü nesil sinir ağı - biyolojik nöronları daha gerçekçi bir şekilde taklit eden spiring nöral ağlar uygulamaları sinir ağı teknolojisinde yeni gelişmeler arasındadır. FPGA (Field Programmable Gate Arrays) ler tarafından sağlanan ve sinir ağlarının hızla gelişmesine ve değişmekte olan tehditlere uyum sağlamalarına olanak tanıyan sistemler siber savunmaya önemli katkılar sağlamaktadır [12].

2) Uzman Sistemler (Expert Systems): Uzman sistemler en çok kullanılan Yapay Zeka araçlarıdır. Uzman sistem, bazı uygulamalarda bulunan etkinlik alanlarındaki, bir kullanıcı veya başka bir yazılım tarafından sunulan soruların yanıtlarını bulmak için kullanılan bir yazılımdır. Tıbbi teşhis, mali veya siber gibi alanlarda kararlara destek sağlamak için doğrudan kullanılabilir. Problemleri çözümleri için küçük teknik teşhis sistemlerinden karmaşık, çok büyük ve sofistike hibrid sistemlere kadar çok çeşitli uzman sistemler bulunmaktadır. Kavramsal olarak, bir uzman sistem, belirli bir uygulama alanı hakkındaki uzman bilginin depolandığı bir bilgi tabanı içerir. Bu bilgi altyapısının yanında, bu bilgiyi temel alan cevaplar elde etmek için bir çıkarsama motoru ve durum hakkında ek bilgilere de sahiptir. Boş bilgi tabanı ve çıkarım motoru, birlikte uzman sistem kabuğu olarak adlandırılır - kullanılabilmesi için, bilgi ile doldurulması gerekir. Uzman sistem kabuğu, bilgi tabanına bilgi eklemek için yazılım tarafından desteklenebilmeli ve kullanıcı etkileşimleri için ve hibrid uzman sistemlerinde kullanılabilecek diğer programlarla genişletilebilir olmalıdır. Uzman sistem geliştirmek, öncelikle, bir uzman sistem kabuğunun seçilmesi / adaptasyonu ve ikincisi, uzman bilgi edinme ve bilgi tabanını bilgiyle doldurma anlamına gelir. İkinci adım, ilk adımdan çok daha karmaşık ve ilkden çok daha fazla zaman almaktadır.

Siber savunmada kullanılabilecek uzman sistemlere örnek güvenlik planlamasıdır [28]. Bu alanda kullanılan bir uzman sistem, güvenlik önlemlerini seçme işini önemli ölçüde kolaylaştırır ve sınırlı kaynakların en iyi şekilde kullanılması için rehberlik sağlar. Ayrıca saldırı tespitinde uzman sistemlerin kullanımı eskilere dayanmaktadır [29, 30].

3) Akıllı Ajanlar (Intelligent Agents): Akıllı ajanlar, akıllı davranışın onu özel yapan (proaktiflik, ajan iletişim dilini anlama ve tepki verme) bazı özelliklerine sahip olan yazılım bileşenidir. Bu yazılım bileşenlerinin planlama, değişkenlik ve derin düşünce kabiliyetleri vardır. Yazılım ajanlarının, proaktif ve ajan iletişim dilini kullanan nesneler olararak düşünüldüğü yazılım mühendisliğinde bir konsept olarak benimsenmiştir. Bununla birlikte ajanlar ve nesneler karşılaştırıldığında, nesnelerin pasif olabileceği ve (iyi tanımlanmış sözdizimi olan iletileri kabul etmesine rağmen) herhangi bir dili anlamaları gerekmediği aradaki farklılıklar olarak gösterilebilir [12].

Akıllı ajanların, siber savunmada kullanılması konusunda DDoS saldırılarına karşı nasıl etkili bir yöntem olduğubu simüle ederek gösteren çalışmalar mevcuttur [31, 32]. Bu çalışmaların bazılarında, bazı yasal ve ticari problemleri çözdükten sonra hareketli akıllı ajanlardan oluşan bir "siber polis" geliştirilmesinin mümkün olduğu da belirtilmektedir [33]. Ayrıca hibrid çoklu ajan ve sinirsel network tabanlı saldırı tespit sistemleri [34] ile ajan tabanlı dağıtılmış saldırı tespit sistemleri [35] bu konuda yapılan diğer bilimsel araştırmalardır.

4) Arama (Search): Arama çeşitli şekil ve biçimlerde hemen hemen her akıllı programda bulunur ve verimliliği genelde tüm programın performansı için kritiktir. Bir çözüm için gereklilikleri yerine getirmekle birlikte, araştırmaya rehberlik etmek için ek bilgi kullanılabiliyorsa, arama etkinliği önemli ölçüde geliştirilebilir. Yapay Zekada birçok arama methodu geliştirilmiş olup birçok yazılımda kullanılmasına karşın genel olarak bu durum Yapay Zekanın kullanımı olarak görülmemektedir. Örneğin, özellikle optimal güvenlik problemlerini çözmede kullanılan dinamik programlamada [36, 37] arama yazılımlar gömülü olup bir Yapay Zeka uygulaması olarak gözükmemektedir. Andor ağaçları (andor trees), αβ-arama, minimax arama ve stokastik arama, oyun yazılımlarında yaygın olarak kullanılmaktadır ve siber savunma için karar verme konusunda kullanışlıdır. Başlangıçta bilgisayar satranç oyunları için geliştirilen αβ-arama algoritması, problem çözmede ve özellikle iki saldırının muhtemel en iyi olası eylemlerini değerlendirip karar verme konusunda oldukça başarılıdır. En az kazanma ve en çok kaybetme tahminlerini kullanan bu algoritma, büyük bir seçenek sayısının göz ardı edilmesi ile aramanın hızlandırılmasını sağlar.

5) Öğrenme (Learning): Öğrenme, bilgi tabanını genişleterek veya yeniden düzenleyerek veya çıkarım motorunu geliştirerek bir bilgi sistemini geliştirmektedir [38]. Makine öğrenimi, yeni bilgileri, yeni becerileri ve mevcut bilgileri organize etmenin yeni yollarını elde etmek için hesaplama yöntemlerini içerir. Öğrenme problemleri, basit parametik öğrenmeden (bazı parametrelerin değerlerini öğrenme ve konseptlerin öğrenimi, dil yapıları, fonksiyonları ve hatta davranış öğrenimi gibi sembolik öğrenmenin karmaşık biçimleri) kaynaklanan karmaşıklıklarına göre büyük farklılıklar göstermektedir. Yapay Zeka hem denetlenmiş öğrenme (öğretmenle öğrenme) hem de denetlenmeyen öğrenme için yöntemler sunar. Denetlenmeyen öğrenme, büyük miktarda verinin bulunması durumunda özellikle kullanışlıdır ve bu yöntem, büyük günlüklerin toplanabileceği siber savunmada yaygındır. Veri madenciliği başlangıçta Yapay Zekada denetlenmeyen öğrenimden çıkmıştır [18, 39].

Seçkin bir öğrenme sınıfı, paralel donanım üzerinde yürütülmesi için uygun olan paralel öğrenme algoritmaları tarafından oluşturulmuştur. Bu öğrenme yöntemleri genetik algoritmalar ve sinir ağları ile temsil edilmektedir. Genetik algoritmalar ve bulanık mantık yöntemleri siber savunma alanında örneğin, tehdit algılama sistemlerinde kullanılmıştır [40].

6) Kısıtlama Çözümü (Constraint Solving): Kısıtlama çözümü veya kısıtlılık doyumu, çözüm üzerinde bir dizi kısıtlama vererek sunulan problemlerin çözümünde (mantıksal ifadeler, tablolar, denklemler, eşitsizlikler gibi) Yapay Zeka kullanılarak geliştirilen bir tekniktir [41]. Bir sorunun çözümü, tüm kısıtlamaları karşılayan değerlerin bir koleksiyonudur (bir dizi). Aslında, kısıtlamaların doğasına bağlı olarak (örneğin, sonlu kümeler üzerindeki kısıtlamalar, işlevsel sınırlamalar, rasyonel ağaçlar) birçok farklı kısıt çözme tekniği vardır. Çok soyut bir seviyede, neredeyse herhangi bir problem bir kısıtlılık doyum problemi olarak sunulabilir. Bu problemlerin çözümü genel olarak çok sayıda aramaya duyulan ihtiyaç yüzünden oldukça zordur. Kısıt çözme, mantık programlama ile birlikte durum analizi ve karar desteklerinde kullanılabilmektedir [42, 43].

IV. SONUÇ (RESULTS)

ABD Savunma Bakanlığı, yayınladığı siber strateji dökümanında, siber savaş ortamı için beş temel ilke belirlemiştir. Bu ilkeler şöyledir [44];

i. Siber alan, yeni bir etkinlik alanı olarak diğer savaş ortamlarına benzer unsurlar taşımaktadır ve dolayısı ile hava, kara, deniz ve uzaydan sonra yeni bir savaş alanı olarak benimsenmelidir.
ii. Pasif savunma yerine proaktif savunmalara geçilmelidir.
iii. Kritik altyapının korunmasını sağlamak için kritik alt yapı koruması (CIP) konsepti adapte edilmelidir.
iv. Müşterek savunmanın, erken tespit kabiliyeti sağlamasına yönelik, savunma yapısına dahil edilmesi için kullanımı sağlanmalıdır.
v. Teknolojik değişim avantajları korunmalı, geliştirilmeli ve yeni teknolojiler (özellikle yapay zeka) siber savunma sistemlerine adapte edilmeldir.

Bu 5 temel ilkeden beşinci ilke özellikle önemlidir. Siber alanın, insanlar tarafından kategori ve idari edilemeyecek kadar büyüklükte veri değerlerine ulaşması, teknolojik gelişmelerin hızı ve bu gelişmelerle birlikte meydana gelen çok daha karmaşık ve sofistike siber tehditler, ve bu tehditlerin doğurabileceği zararları en aza indirgeyebilmek adına olabildiğince erken tespit edilmesi ve önlenmesi gibi

durumlar yapay zekayı siber savunmanın vazgeçilmez bir unsuru kılmıştır.

Gelecek çalışma konusu olarak siber savunma için kullanılmak istenen yapay zeka teknolojilerinin siber savunma tatbikatlarına entegre edilmesi ve kullanılması konusu seçilmiştir.

V. KAYNAKLAR(REFERENCES)

[1] S. Dilek, H. Çakır, M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", 2015.

[2] R. High, "The Era of Cognitive Systems: An Inside Look at IBM Watson and How it Works", IBM, 2012.

[3] J. E. Kelly, "Computing, Cognition and the Future of Knowing", IBM, 2015.

[4] J. Dean, "Large-Scale Deep Learning for Intelligent Computer Systems", 2016.

[5] K. Veeramachaneni, I. Arnaldo, A. Cuesta-Infante, V. Korrapati, C. Bassias, K. Li, "AI2: Training a Big Data Machine to Defend", IEEE International Conference on Big Data Security in New York City, 2016.

[6] I.Kotenko, "Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007.

[7] M. Golling, B. Stelte, "Requirements for a Future EWS Cyber Defence in the Internet of the Future", 3rd International Conference on Cyber Conflict, CCD COE, 2011.

[8] A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Junior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review", Journal of Network and Computer Applications, Elsevier, 2013.

[9] S. Edelkamp, C. Elfers, M. Horstmann, M. S. Schröder, K. Sohr, T. Wagner, "Early Warning and Intrusion Detection based on Combined AI Methods", 2009.

[10] A. Patel, Q Qassim, Z. Shukor, J. Nogueira, J Júnior, C. Wills, "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System, Proceedings of the South African Information Security Multi-Conference", Port Elizabeth, South Africa, 2010.

[11] J. Helano, M. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", the International Journal of Forensic Computer Science, 2006.

[12] E. Tyugu, "Artificial Intelligence in Cyber Defense", 3rd International Conference on Cyber Conflict, 2011.

[13] J. S. Russell, P. Norvig, "Artificial Intelligence: A Modern Approach", 2nd edition, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003.

[14] G. Luger, W. Stubblefield, "Artificial Intelligence: Structures and Strategies for Complex Problem Solving", Addison Wesley. 2004.

[15] F. Rosenblatt. "The Perceptron - A Perceiving and Recognizing Automaton", Cornell Aeronautical Laboratory, 1957.

[16] Y. A. Freund, R. E. Schapire, "Large Margin Classification Using the Perceptron Algorithm, Machine Learning", 37(3):277-296, 1999.

[17] G. 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.

[18] J. Bai, Y. Wu, G. Wang, S. X. Yang, W. Qiu, "A Novel Intrusion Detection Model Based on Multilayer Self- organizing Maps and Principal Component Analysis, Advances in Neural Networks", ISNN Springer Berlin Heidelberg, 2006.

[19] F. Barika, K. Hadjar, N. El-Kadhi, "Artificial Neural Network for Mobile IDS Solution", Security and Management, 2009.

[20] D. A. Bitter, T. Elizondo, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence, CCIB, Barcelona, Spain, 2010.

[21] R. I. Chang, L. B. Lai, W. D. Su, J. C. Wang, J. S. Kouh, "Intrusion Detection by Backpropagation Neural Networks with Sample-query and Attribute-query", International Journal of Computational Intelligence Research, 2007.

[22] B. Iftikhar, A. S. Alghamdi, "Application of Artificial Neural Network in Detection of DOS Attacks", Proceedings of the 2nd international Conference on Security of Information and Networks. New York, NY, 2009.

[23] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of Artificial Neural Networks Techniques to Computer Worm Detection", International Joint Conference on Neural Networks, 2006.

[24] C. H. Wu, "Behavior-based Spam Detection Using a Hybrid Method of Rule-based Techniques and Neural Networks", Expert Systems with Applications, 2009.

[25] P. Salvador, et al., "Framework for Zombie Detection Using Neural Networks", Fourth International Conference on Internet Monitoring and Protection, 2009.

[26] M. Shankarapani, K. Kancherla, S. Ramammoorthy, R. Movva, S. Mukkamala, "Kernel Machines for Malware Classification and Similarity Analysis", IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010.

[27] B. Fei, J. Eloff, M. S. Olivier, H. Venter, "The Use of Self-organizing Maps of Anomalous Behavior Detection in a Digital Investigation", Forensic Science International, 2006.

[28] J. Kivimaa, A. Ojamaa, E. Tyugu, "Graded Security Expert System", Springer, 2009.

[29] D. Anderson, T. Frivold, A. Valdes, "Next-generation Intrusion Detection Expert System (NIDES)", SRI International, Computer Science Lab, 1995.

[30] T. F. Lunt, R. Jagannathan, "A Prototype Real-Time Intrusion-Detection Expert System", IEEE Symposium on Security and Privacy, 1988.

[31] I. Kotenko, A. Ulanov, "Multi-Agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks", International Workshop on Autonomous Intelligent Systems: Agents and Data Mining, Springer.

[32] I. Kotenko, A. Konovalov, A. Shorov, "Agent-Based Modeling and Simulation of Botnets and Botnet Defence", Conference on Cyber Conflict, CCD COE Publications, Tallinn, Estonia, 2010.

[33] 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", IEEE World Congress on Computational Intelligence, Barcelona, Spain, 2010.

[34] E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid Multi Agent-neural Network Intrusion Detection with Mobile Visualization", Innovations in Hybrid Intelligent Systems, 2007.

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

[36] J. Kivimaa, A. Ojamaa, E. Tyugu, "Pareto-Optimal Situation Analysis for Selection of Security Measures", MilCom, 2008.

[37] J. Kivimaa, A. Ojamaa, E. Tyugu, "Managing Evolving Security Situations", MilCom, 2009.

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

[39] V. K. Pachghare, P. Kulkarni, D. M. Nikam, "Intrusion Detection System using Self Organizing Maps", International Conference on Intelligent Agent & Multimedia Agent Systems, 2009.

[40] R. Hosseini, J. Dehmeshki, S. Barman, M. Mazinani, S. Qanadli, "A Genetic Type-2 Fuzzy Logic System for Pattern Recognition in Computer Aided Detection Systems", IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010.

[41] B. Mayoh, E. Tyugu, J. Penjam, "Constraint Programming", NATO ASI Series, Springer Verlag. 1994.

[42] I. Bratko, "PROLOG Programming for Artificial Intelligence", Addison-Wesley, 2001.

[43] X. Ou, "A Logic-programming Approach to Network Security Analysis", PhD Thesis, Princeton University, 2005.

[44] "US Department of Defense Cyber Strategy", US DoD, April 2015.