YAPAY ZEKA VE GELECEĞİN SİBER SAVAŞLARI

Dr. Öğr. Üyesi Utku KÖSE [*Süleyman Demirel Üniversitesi, Bilgisayar Mühendisliği Bölümü*


Yapay zekâ ile örülü bir gelecek
insanlığın çoktan beri beklediği bir sonuç.
Peki, siber güvenlik ve ilgili konular
yapay zekânın gölgesi altında nasıl gelişecek?
Zeki sistemlerin baskın olabileceği bir
gelecekte siber güvenliğin kaderi
ne olacak?

Günümüzün ve geleceğin en önemli bilim ve teknoloji alanlarından birisi olan yapay zekânın geçmişi 1950'li yıllara kadar uzansa da günlük hayatımızda yer edinmeye başlaması özellikle son 10 yılda ivme kazandı. Bugün, akıllı telefonlarımızdan günlük hayatta etkileşime girdiğimiz cihazlara ve hatta iş süreçlerinde kullanılan veri odaklı yazılımlara kadar birçok ortamda yapay zekânın gücünden faydalanıyoruz. Yapay zekâ robotlar gibi donanımsal sistemleri zorunlu kılmaz, diğer bir deyişle, zeki çözümlemeler içeren yazılımlar da yapay zekâ tabanlı olabilir. Bu teknolojinin önlenemez yükselişi öyle bir aşamaya geldi ki artık yapay zekânın başarılı çözümler üretmediği herhangi bir alan neredeyse yok gibi. Mühendislik odaklı alanlardan tıbba, eğitimden ekonomiye ve hatta edebiyat ile sanata kadar birçok farklı alanda yapay zekâ uygulamalarını görüyoruz.

Bilgisayar teknolojisinin gelişimiyle beraber siber güvenlik alanı da gelişiyor. Siber saldırı ve siber savunma yaklaşım, yöntem ve teknikleri karşılıklı olarak sürekli değişiyor ve yapay zekâ gibi geleceğin bilim alanlarının da bu değişimde aktif rol alacağı açıkça görülüyor. Günümüzde siber savaş ve siber terör gibi kavramlar sıklıkla kullanır hâle geldi, öyle ki devletler düzeyinde bile bu konuda alınacak önlemler hakkında fikirler ortaya konuluyor.

Bu noktada, fiziksel savaşların yerini giderek siber savaşlara bırakacağını ifade edebiliriz. Ancak madalyonun diğer yüzünde yapay zekâ var. Yani, yapay zekâ tabanlı bir siber savaşın nasıl olabileceği ve zeki sistemlerin siber saldırı ve savunma aşamalarında ne gibi roller alabileceğini öngörebilmemiz gerekiyor. Ayrıca, öngörülerimizin mevcut yapay zekâ gelişmeleri ve muhtemel ilerlemeler ile tutarlı bir kapsamda ortaya konulması da son derece önemli.

Yapay Zekâ Nedir?

Yapay zekâyı bilgisayar bilimleri altında gerek donanımsal gerekse sadece yazılımsal zeki sistemlerin tasarlanıp geliştirilmesi ile ilgilenen bir alan olarak tanımlayabiliriz. Yine gerçek dünya tabanlı problemleri çözmek için çeşitli yapay zekâ yaklaşım, yöntem ve teknikleriyle geliştirilmiş yazılımlara da yapay zekâ diyebiliriz. Bu teknolojinin amacı, sayısal sistemler üzerinden gerçek dünya problemlerinin çözülmesi amacıyla zeki sistemlerin oluşturulması. Bunu sağlayan da bünyesinde çeşitli matematiksel ve mantıksal yapılar barındıran özel algoritmalar. Tarihsel süreç, yapay zekâ algoritmalarının başta insan olmak üzere, çeşitli canlılardan (örneğin; hayvanlar, böcekler) ve hatta doğadaki rutin dinamiklerden esinlenerek oluşturulmasına sahne olmuş. Hâlen de bilimsel araştırmalar bu yönde ilerliyor.

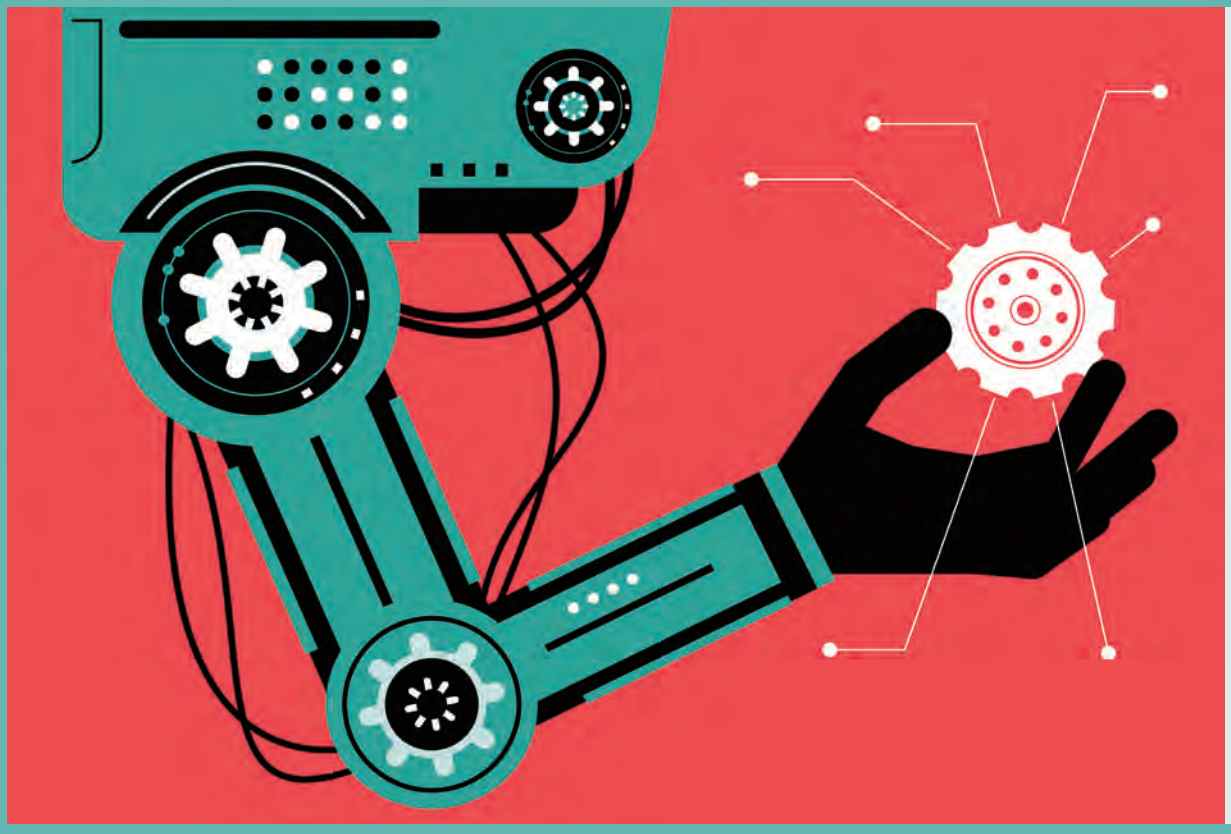
Yapay Zekâ Nasıl Çözüm Üretir?

Yapay zekâ algoritmaları, ustaca bir araya getirilmiş mantıksal ve matematiksel adımların yanında, bazı temel yollara bağlı kalarak çalışır. Eldeki veriler üzerinden çok sayıda (10.000, 100.000, belki de daha fazla) döngüyle çözüm üretme, verileri manipüle etme ya da bilinen çözümlerden yola çıkarak bilinmeyenlere adapte olma bunlardan en önemlisi. Yapay zekânın uygulanma biçimlerine ve hedef problemlerine göre çok sayıda alt alanı bulunur.

Öğrenmeye ihtiyaç duymayan yapay zekâ algoritmaları, problemimizi mevcut algoritmik adımlarla doğrudan çözebilen algoritmalardır. En basitinden, optimizasyon için kullanılan ve kuşlar, balıklar, arılar ya da karıncalardan esinlenerek geliştirilmiş olan sürü zekâsı algoritmaları, hedef problemin matematiksel modeli üzerinden hemen çözüme ulaşabilir. Ancak bazı gerçek dünya tabanlı problemler, geçmiş tecrübelerden ve bazı bilinenlerden faydalanılarak çözülebilir. Bu durum, biz insanların tecrübelerden öğrenmesi ve problemleri böylelikle çözümlemesi ile benzeşir. Öğrenmeye ihtiyaç duyan yapay zekâ algoritmaları bunun üzerine kurulu olarak tasarlanmıştır. Makine öğrenmesi (machine learning) alt alanı içerisinde incelenen bu algoritmalar, geleceğin yapay zekâ sistemlerinin temelini oluşturmakla birlikte, bu yazının konusu olan geleceğin siber savaşlarını da yakından ilgilendirir.

Yapay Zekâ Teknolojisindeki Başarının Sırları:

- Yapay zekâ mantıksal ve matematiksel yönden güçlü algoritmalara dayanır.
- Yapay zekâyı oluşturan algoritmalar, farklı problemlere uygulanabilecek düzeyde esnek yapılara sahip. Günümüzde yapay zekâ algoritmaları bir arada kullanılarak daha güçlü hibrit yapay zekâ sistemleri de elde edilebiliyor.
- Yapay zekâ kapsamındaki algoritmaların, tahmin etme, yorumlama, optimize etme, adaptif bir biçimde kontrol edebilme ve genel anlamda öğrenerek ilerleyebilme gibi yetenekleri var. Bu durum, özellikle gerçek dünya tabanlı problemleri çözmek için oldukça önemli.
- Yapay zekâ, çözülmesi uzun zaman alan, yanlış çözümlenen ya da çözülmesi imkânsız olan problemleri hızlı ve etkin bir biçimde çözebilir.



Makine Öğrenmesi ve Siber Güvenlik

Makine öğrenmesi, aslında bütün bu yapay zekâ tartışmalarının ve hatta ortaya çıkan çeşitli endişelerin (zeki makinelerin insanlığı ele geçirme ihtimali, işsizliğe sebep olabilmeleri vb.) kaynağı durumundaki yapay zekâ tekniklerini içerir. Bu teknikler, hedef probleme uygulanmadan önce çeşitli eğitim verileri üzerinde öğrenme süreci geçirmesi gereken algoritmalardır. Bu açıdan baktığımızda tipik bir makine öğrenmesi algoritması / tekniği, sırasıyla öğrenme, test ve uygulama süreçlerinden geçer. Öğrenme, algoritmanın eğitimine; test süreci, gerçek uygulama öncesi algoritmanın tekrar eğitime ihtiyaç duyup duymadığının değerlendirilmesine ve nihayetinde uygulama süreci de eğitilmiş algoritmanın artık pratikte de kullanılmasına karşılık gelir. Bütün bu mekanizma, bizleri otonom zeki sistemlere götürür. Gelecek, günlük hayatımızda bizlere yardımcı olacak veya arka planda veriler üzerinde hızlı işlemler gerçekleştirecek bu tür zeki sistemlerle dolu olacak.

Makine Öğrenmesinin Siber Güvenliğe Adaptasyonu

Siber güvenlik konusu, başta bilgisayar ve iletişim teknolojileri olmak üzere, farklı teknolojilerin gelişimiyle birlikte iyice karmaşıklaşan bir problem hâline geldi. İnsan hayatının gerçek dünyadan siber ortama iyiden iyiye kayması süreci, siber güvenliğin zaman ilerledikçe kritikleşmesine sebep oldu. Bugün ortalama bilgisayar kullanıcılarının birçoğu farkında olmadan siber güvenlik tehdidiyle karşı karşıya kalıyor. Ayrıca, siber saldırıların sosyal mühendislik gibi hayatın içinde yer alan ve insan psikolojisiyle ilişkili manipülatör eylemlerle desteklenmesiyle de insanların çeşitli problemlerle karşı karşıya kalması kaçınılmaz oluyor. Hâlihazırda uzmanlığı önemli birikimler ve tecrübeler gerektiren siber güvenlik, yapay zekânın süreçlere dâhil olmasıyla birlikte farklı boyutlara taşınmış durumda. Bu noktada, kendi kendini geliştirebilen makine öğrenmesi teknikleri, hem siber saldırı tarafında hem de siber savunma tarafında oldukça önemli roller üstleniyor.

Makine Öğrenmesi Siber Güvenlik Odaklı Faaliyetlere Nasıl ve Neden Adapte Olur?

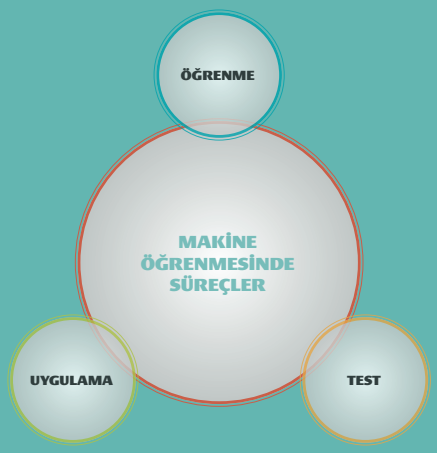
1. Siber saldırı ve savunma faaliyetleri algoritmiktir. Yani, bilgisayar programlamanın ötesinde, her bir faaliyeti belli işlem adımları içerisinde plana dökmek mümkün. Yapay zekâ da algoritmik adımların üstadı olarak bu tür süreçleri çok iyi simüle edebilir.

2. Nasıl ki bir hacker (korsan veya etik nitelikte), belirli eğitim süreçlerinden geçerek kendini geliştirebiliyorsa saf bir makine öğrenmesi algoritması, gerekli uzman bilgilerinin ve yaparak öğrenme süreçlerinin gerçekleştirilmesiyle zeki bir hacker sistemi hâline dönüştürülebilir. Ayrıca bu süreç, bilgisayar tabanlı sistemlerin avantajları sayesinde bir insandan çok daha kısa sürede gerçekleştirilebilir.

3. Tipik bir yapay zekâ sistemi, biz insanlar gibi verileri anlamlandırmaya ve detaylandırmaya ihtiyaç duymadan, gizli örüntüleri ortaya çıkararak doğrudan işine yarar hâle getirebilir. Yapay zekâ zaten bu yönüyle öne çıkar ve insan kapasitesinin üstünde başarılar ortaya koyabilir.

4. Artan veri karmaşıklığı ve büyüklüğü, siber savunma faaliyetlerini olduğu kadar siber saldırı faaliyetlerini de zorlaştırır. Dolayısıyla aynı anda çok sayıda veriye hükmedebilecek ve söz konusu karmaşıklıkta insanların iş yükünü rahatlatacak sistemler mevcut koşullar altında ancak yapay zekâ tabanlı olabilir.

5. Yapay zekâ diğer teknolojik faaliyet alanlarında yayıldıkça siber güvenlik de bundan etkilenir.



Makine Öğrenmesinde Süreçler

Siber saldırı ve savunma faaliyetlerinin hem teorik hem de pratik anlamda makine öğrenmesi teknikleri / algoritmaları ile desteklenmesi oldukça mümkün. Çünkü kaotik yapıdaki problemlere bile çözümler üretebilen yapay zekânın, aslında büyük resimde algoritmik faaliyetleri içeren hacking, cracking ve bağlı faaliyetlerin üstesinden gelmesi oldukça kolaydır.

Makine Öğrenmesindeki Yaklaşımlar

Danışmanlı Öğrenme *(Supervised Learning)*
Bu yaklaşımda, algoritma, bilinen problem verileri ve bunların karşılığında nasıl sonuçlar elde edilebildiğini gösteren bir veri seti ile eğitilir.

Danışmansız Öğrenme *(Unsupervised Learning)*
Danışmansız öğrenme yaklaşımında yine eğitim veri seti vardır. Ancak bu veri setinde bilinen problem verileri olmasına karşın bunlardan elde edilebilecek sonuçlar bilinmemektedir. Dolayısıyla algoritma / teknik veriler üzerinden geçerken sonuçlara yönelik sınıflandırmayı kendisi yapar.

Takviyeli Öğrenme *(Reinforcement Learning)*
Takviyeli öğrenme yaklaşımında algoritmanın elde ettiği bir çözüm karşısında bu çözümün iyi mi kötü mü, doğru mu yanlış mı olduğuna ilişkin dönütler verilir. Algoritma bu şekilde eğitilir ve öğrenir.

Yarı Danışmanlı Öğrenme *(Semi-Supervised Learning)*
Bu öğrenme yaklaşımı danışmansız öğrenme ile danışmanlı öğrenme ara-sındadır.

Bu öğrenme yaklaşımlarından yola çıkarak, "saf" yapıda bir zeki sistemin, dışarıdan maruz kaldığı veriler neticesinde kendini geliştirmesi ve belirli bir yönde ilerlemesi mümkün. Ancak burada ilk akla gelen şey, gelişen teknoloji neticesinde oldukça gelişmiş makine öğrenmesi yani yapay zekâ tabanlı sistemlerin nelere sebep olabileceğidir. Siber güvenlik konusu da bu durumdan etkilenecekler arasında ön sıralarda yer alır.

Geleceğin Siber Savaşları İçin Yapay Zekâ Tabanlı Sistemler

Şu ana kadarki açıklamalarımız ile bağlantılı olarak, geleceğin siber savaşlarını yönlendirecek yapay zekâ tabanlı sistemler konusunda çeşitli tahminlerde bulunabiliriz. Burada önemli olan husus, gelecekte çok daha yoğun miktarda veri akışı ve gerçek hayat üzerinde çok daha fazla baskın konuma ulaşacak siber dünyanın olacağıdır. Günümüzde hepimizin dikkatini çeken bir husus da teknolojinin bizleri gittikçe kendine bağlamasıdır. Bunun sebebi siber dünyanın günlük hayatımızı gittikçe kolaylaştırması ve bizleri oyalamasıyla siber dünyada gerçek hayattan daha fazla zaman harcamamızdır. Görünen o ki bu süreç yapay zekânın istikrarlı ilerlemesi neticesinde çok daha kritik bir hâle gelecek.

Rol Tabanlı Zeki Sistemler

Geleceğin siber savaş ortamında yer alacak zeki sistemler, muhtemelen rol tabanlı olacak. Fiziksel bir savaşta çeşitli rollerde unsurlar (askerler, zırhlı araçlar, hava, kara veya deniz araçları ve benzeri) bulunduğu gibi, siber saldırı ve savunma stratejilerinin oluşturulabilmesi adına, geleceğin zeki sistemleri de kendi içlerinde rol dağılımlarına gidebilir. Bu noktada, daha önce de değindiğimiz etmen tabanlı mimariye sadık kalınabileceği gibi, şu anda öngöremediğimiz mimari yapılarda zeki sistemler de sürece dâhil olabilir.

Siber Güvenlik Yönelimli Bir Zeki Sistem Nasıl Elde Edilir?

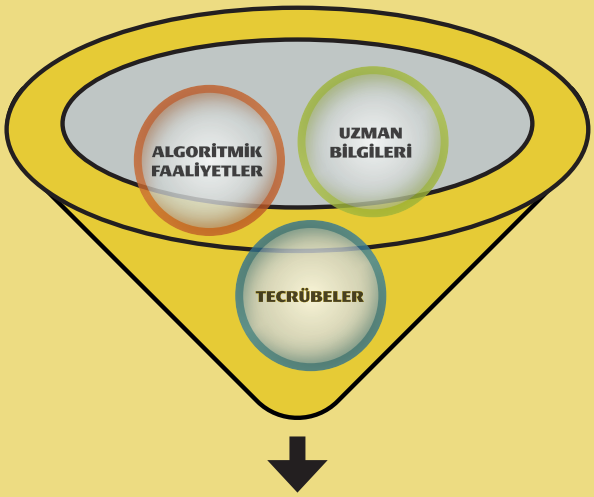
- Siber saldırı ve güvenlik faaliyetleri gerçekleştiren kişilerin görüşlerinin modellenmesi sonrasında, bu modellenmiş görüşlerden beslenen zeki yazılımlarla, mevcut durumda kullanılan donanımsal ve yazılımsal araçların yapay zekâ tabanlı optimum kontrolü sağlanabilir.

- Yine ilgili kişilerin tecrübeleri uygun yaklaşımlarla modellendiği takdirde, zeki bir hacker yazılımı geliştirilebilir. Bu yazılım, makine öğrenmesi tabanlı olmakla birlikte, saldırı ve savunma amaçlı eğitilebilir, hatta otonom faaliyet göstererek insanlardan bağımsız olarak işler hâle gelebilir.

- Yapay zekânın popüler konularından olan etmen (agent-ajan) tabanlı sistemler aynı anda farklı görevlerdeki, ufak ama etkili zeki sistemlerin gerçekleştirilmesine olanak sağlar. Etmen tabanlı mimari sayesinde bu sistemlerin kolektif bir saldırı / savunma ağı (etmen sürüsü) kurması mümkün hâle gelir.

- Yapay zekâ büyük miktardaki verilerden anlamlar çıkarabilme ve hatta sürece ait kaotik zaman serilerinden gelecek süreci tahmin edebilme yeterliğine sahiptir. Bu sayede çok daha hassas siber savunma sistemleri, öte yandan da çok daha sinsi ve esnek siber saldırı sistemleri geliştirilebilir.

- Virüs, Truva atı (trojan) ya da solucan (worm) gibi farklı saldırı araçlarının özellik ve işlevlerinden çok daha fazlasını simüle edebilecek, tespiti neredeyse imkânsız kötü amaçlı yazılımlar ortaya konulabilir. Benzer şekilde bunları tespit edecek ve hatta yok edecek sistemlerin de yapay zekâ tabanlı olması gerekir.



Yapay zekâ tabanlı siber güvenlikte rol oynayan temel unsurlar.

Saldırı - Savunma Sınıfları ve Kolektif Bilinç

Rol dağılımları daha genel çerçevede saldırı ve savunma görevlerini yerine getirecek iki ayrı sınıf altında toplanabilir. Yani bir grubu (örneğin bir ülkeyi) temsil eden tipik bir zeki sistem ordusu, aslında saldırı ve savunma hattı olmak üzere iki sınıf altında şekillenecektir. Dolayısıyla hem saldırı hem de savunma sınıfında merkezi yapay zekâ mevcut olacak, bunun yanında iki farklı sınıf siber savaş olsun veya olmasın sürekli iletişim hâlinde olacaklardır. Anlaşılacağı üzere, saldırı ve savunma odaklı asker sistemler arasında, algoritmik hareket mantıkları açısından birtakım farklılıklar olabilecek, merkezi yapay zekâ sistemleri de saldırı ya da savunma sınıfından hangisine ait ise o yönde kendi sınıfını eğitme, yönlendirme ve genel bağlamda yönetme kapasitesine sahip olacaklardır.

Rol dağılımları ve sınıflar kapsamında, geleceğin siber savaş donanımlı zeki sistemlerindeki en önemli mekanizma, kuşkusuz ki kolektif bir bilinç üzerine kurulu olacaktır. Söz konusu kolektif bilinç, güvenlik ve zafiyet endişeleri nedeniyle kısıtlanacak bazı zeki sistemler (asker sistemler, işçi sistemler) haricinde bütün yapay zekâ tabanlı zeki sistemler arasında var olacak bir iletişim sistemine karşılık gelecektir. Asker sistemler ve işçi sistemler gibi zeki sistemler de kendi aralarında farklı boyutlarda kolektif bilinç oluşturabilecektir. Kolektif bilinç, esasında bütün zeki sistemleri yöneten, kendi kendine değişen ve yok edilmesi ancak ve ancak bütün ordunun ortadan kaldırılmasıyla mümkün olabilecek bir sistem olacaktır.

Hiyerarşik Zeki Sistemler

Günümüz yapay zekâ sistemleri yetenekleri ve kurulu oldukları problem çözüm yapısının karmaşıklık düzeyine göre farklı düzeylerde olabiliyor. Benzer şekilde, sahip oldukları yeterlikleri ve güçleri itibariyle geleceğin siber savaşlarında yer alacak zeki sistemlerin de hiyerarşik bir düzene sahip olacağı öngörülüyor. Ancak bunun sebebi sadece sahip olunan yeterlikler değil, aynı zamanda siber savaş düzeyinde sahip olunan yetki düzeyleri olacaktır. Özellikle siber güvenlik gibi temelinde güven unsurunun şart koşulduğu bir düzen içerisinde yetkiler -bildiğimiz üzere- son derece kritiktir. Buradan hareketle, geleceğin otonom siber savaşlarının da hiyerarşik düzeyde, yetki düzenlerine uyan zeki sistemlerle gerçekleşeceğini söylemek yanlış olmaz.

Sayısal Diller ve Kriptoloji Savaşları

Geleceğin siber savaşları, insan yeteneklerinin çok üstünde, özellikle süper zekâ tabanlı zeki sistemlerin rol alacağı savaşlar olarak sürebilir. Temel aktörlerin ileri düzey yapay zekâ tabanlı sistemler olacağı böyle bir ortamda, saldırı ve savunma süreçlerinin en üst düzeyde meydana gelmesi adına, söz konusu zeki sistemlerin kendi içerisinde çeşitli sayısal diller geliştireceğini de öngörmek mümkündür.

Sayısal dillerden kastımız, aynı orduda-tarafta yer alan sistemlerin kendi aralarında iletişim sürecini yerine getirebilecekleri, uygulanan stratejilere ve gerçekleştirilen faaliyetlere yönelik bilgileri birbirlerine aktarmalarını sağlayacak, esnek ve değişken sayısal kodlardır.

Durumu biraz daha ileriye götürmek gerekirse, geleceğin otonom siber savaş ortamlarında kazananı ve kaybedeni belirleyen temel unsurlardan birisinin de kriptoloji savaşları olacağını öngörebiliriz. Bu bağlamda, günümüzde kırılması çok zor şifreleme yapılarının çok çok ötesinde, yapay zekâ sistemleri tarafından üretilen üstün şifreleme ve şifre çözme tekniklerinin, siber saldırı ve savunma faaliyetlerinin kaderini belirleyecek ve sürekli kullanılacak unsurlar olacağını söyleyebiliriz. Esasında insanlığın geleceğinin veri akışıyla imtihanı ve gelecekte güvenli bir ortam sağlanması temelde "bilginin şifrelenmesi ve gizlenmesi" düsturuna bağlıdır.

Siber Savaşlar - Büyük Veri - Nesnelerin İnterneti

Yapay zekâ ile dolu bir geleceğin eşiğinde özellikle yoğun miktarda veriyle baş edebilmek temel araştırma konuları arasına girmiştir. Bu kapsamda, sıklıkla dile getirilen yoğun veri akışı, büyük veri (big data) adı verilen bir kavram altında incelenmektedir. Tahmin edileceği üzere, geleceğin siber savaşları da büyük veri kapsamında incelenebilecek yoğun veriler çerçevesinde gerçekleşecektir. Yine geleceğin otonom-yapay zekâ içeren siber savaşları, günümüzün yükselen teknolojilerinden olan nesnelerin interneti (internet of things) kapsamında dikkate alınan zeki makineler öncülüğünde sahne alacaktır. Çünkü yapay zekâ tabanlı bir gelecek, zeki makinelerin (örneğin robotların) hayatın her köşesinde yer aldığı bir geleceğe doğru sürüklenmektedir. Dolayısıyla geleceğin siber savaşları, bu tür zeki makinelerin de yeri geldikçe sürece dâhil olduğu, siber dünyada olduğu kadar, gerçek dünyayı da ilgilendiren savaşlara dönüşebilecektir. Fiziksel savaşların yerini alacak siber savaşların, gerçek dünyayla teması belki de sadece bu şekilde söz konusu olacaktır.

İnsanlığı nasıl bir geleceğin beklediği hâlen büyük bir muamma. Ancak günümüzde günlük hayatı şekillendirecek ve yönlendirecek aşamaya gelmiş bazı bilimsel ve teknolojik alanlar geleceğe de göz kırpmaktadır. Yapay zekâ bu alanlardan biri olarak siber güvenlik konusuyla da yakından ilgilidir. Gittikçe siber dünyaya bağlanan insanlık için siber güvenlik ve bağlı konular yapay zekâ nedeniyle çok daha kritik bir hâle gelecektir. Nitekim geleceğin siber savaşlarını yapay zekâ tabanlı zeki sistemlerden bağımsız düşünmek olanaksız. Özellikle kendi kendine öğrenebilme yeteneğine sahip ve algoritmik olduğu kadar matematiksel modellenebilen problemlerle çok kolay başedebilen makine öğrenmesi odaklı algoritmalar / teknikler, bu tür otonom savaşların başlıca aktörleri olacak gibi görünüyor. Bu aşamada gelecekte ne gibi zeki sistemlerin hayatımızda rol oynayacağı ve siber savaşlara hangi formlarda dâhil olacakları bizler için büyük bir sürpriz olabilir. Ancak bu yazıda ifade edilenlerin, günümüz koşulları ve geleceğe dair birtakım işaretler neticesinde, geleceğin siber savaşları hakkında önemli ipuçları barındırdığı muhakkak. ■

Kaynaklar

Copeland, J. *Artificial Intelligence: A Philosophical Introduction*, John Wiley & Sons, 2015.

Göranzon, B.ve Josefson, I., *Knowledge, Skill and Artificial Intelligence*, Springer Science & Business Media, 2012.

Bahrammirzaee, A., "A comparative survey of artificial intelligence applications in finance: artificial neural networks, expert system and hybrid intelligent systems", *Neural Computing and Applications*, Cilt 19, Sayı 8, s.1165-1195, 2010.

Çiftçi, H., *Her Yönüyle Siber Savaş*, TÜBİTAK Popüler Bilim Kitapları, 2013

Ertel, W., *Introduction to Artificial Intelligence*, Springer, 2018.

Nabiyev, V. V.,*Yapay Zekâ*, Seçkin Yayıncılık, 2005.

Mitchell, T. M., *Machine Learning*, McGraw-Hill Science, 1997.

Alpaydin, E., *Introduction to Machine Learning*, MIT Press, 2014.

Shanahan, M., *The Technological Singularity*, MIT Press, 2015.

Yampolskiy, R. V., *Artificial Superintelligence: A Futuristic Approach*, CRC Press, 2015.

John Walker, S., *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Taylor & Francis, 2014.

Wortmann, F. ve Flüchter, K.," Internet of things", *Business & Information Systems Engineering*, Cilt 57, Sayı 3, s. 221-224, 2015.