بسم الله الرحمن الرحيم

Gelecekteki Dünya Savaşı: Bir Sonraki Dünya Savaşı Görünmez Bir Savaş mı Olacak?

Tarihin tanıklık ettiği büyük savaşlarda, her zaman görülebilecek bir şey vardı. Zira Birinci Dünya Savaşı'nda ordular sınırları aşarak harekete geçmiş; cepheler siperler ve toplarla dolup taşmıştı. İkinci Dünya Savaşı'nda ise bizzat şehirler savaş alanlarına dönüşmüş ve savaşın patlak vermesi, insanların zihninde uçakların sesi, sirenler ve düşen bombalarla özdeşleşmişti.

Peki ya savaşın ilk alametleri çalışmayan bir banka ekranı, çöken bir elektrik şebekesi, sistemlerini devreye sokamayan bir havaalanı, devre dışı kalan bir liman ve milyonlarca insanın iletişiminin kesilmesi olsaydı nasıl olurdu acaba?

Bu, gelecekteki dünya savaşının tamamen elektronik olacağına ya da tankların ve füzelerin ortadan kalkacağına dair bir kehanet değildir; ancak ciddiye alınmayı hak eden bir varsayımdır: Zira gücün doğası değişebilir, dolayısıyla savaşların başlama şekli de değişebilir; çünkü devlet artık sadece sınırlardan ve ordulardan ibaret olmadığı gibi modern devlet de sadece bir toprak, ordu ve başkentten ibaret değildir; aksine bankalar, enerji, iletişim, uydular, limanlar, ulaşım, fabrikalar, tedarik zincirleri, su ve gıda sistemleri ile bilgiden oluşan bir birbirine bağlı devasa sistemler ağıdır.

Bu karşılıklı bağımlılık, ülkelere benzeri görülmemiş yetenekler kazandırdı, ancak aynı zamanda benzeri görülmemiş zayıflıklar da yarattı; Gerçek zamanlı çalışan bir ekonomi, temel halkalarından biri bozulursa durma noktasına gelebilir; dijital sistemlere dayanan bir liman, tek bir vinç bile vurulmasa işlevsiz hale gelebilir; milyonlarca müşteriye hizmet veren bir banka ise, kimse tarafından kullanılamayan sağlam bir binaya dönüşebilir.

Avrupa Birliği Siber Güvenlik Ajansı, dijital bağlantılılığın saldırı yüzeyini genişlettiğini ve ortak bağımlılık noktalarının istismar edilmesinin saldırıların tedarik zincirleri boyunca etkisini katlayabileceğini vurgulamaktadır. Ayrıca en son raporları da kamu yönetimi, ulaşım, dijital altyapı ve finans sektörlerinin hedef alınmaya devam ettiğine işaret etmektedir.

İşte burada; şehri vurmaktan ziyade onun damarlarının vurulması gibi hedef alma mefhumu değişmektedir; zira geleneksel bir savaşta, devletin damarlarını kesmek, yolları, köprüleri ve limanları tahrip etmek ya da şehirleri kuşatmak anlamına geliyordu; ama bugün devletin görünmez damarları da vardır; zira internet bir damardır, enerji bir damardır, finans sistemi bir damardır, uydular bir damardır ve tedarik bir damardır; hatta deniz tabanı bile bu denklemin bir parçası haline gelmiştir. Çünkü denizaltı kabloları kıtalararası veri trafiğinin büyük bir bölümünü taşırken diğer bazı denizaltı altyapıları da enerji taşımaktadır. Bunların korunması artık doğrudan bir güvenlik meselesi hâline gelmiştir; bu yüzden NATO, gemi hareketlerini analiz etmek ve deniz altındaki altyapıya yönelik bir tehdide işaret edebilecek davranışları tespit etmek için yapay zekâ kullanan araçlar geliştirmiştir.

İronik olan ise, küresel ekonomideki en önemli yapıların, insanların bilincinden en çok kaybolan şeyler olabilmesidir. Çünkü biz parayı transfer

etmemizi sağlayan kabloyu görmüyoruz, limanı fabrikaya bağlayan sistemi görmüyoruz, hastanenin çalışmasını sağlayan ağı görmüyoruz, ancak durduğu anda değerini anlıyoruz. Yani patlamaya ihtiyaç duymayan bir silah! İşte bu yüzden gelecekteki savaş, sonuçları açısından değil, şekli açısından farklı olabilir.

Finans sektörüne yönelik geniş çaplı bir siber saldırı, parayı çalmaktan ziyade para akışında kaos yaratabilir; ulaşım sistemlerinin devre dışı bırakılması limanı tahrip etmeyebilir ama gemilerin ve eşyaların hareket etmesini engelleyebilir. Bir elektrik şebekesinin hacklenmesi tek bir santralı bile yakıp yıkmayabilir ama şehirleri enerjiden mahrum bırakabilir; iletişim altyapısına yönelik bir saldırı ise doğrudan bir insanı öldürmeyebilir ancak bütün bölgeleri devletten ve dünyadan izole edebilir. İşte burada savaşta yeni bir kural ortaya çıkmaktadır: Silah görünmez olabilir ancak etkisi son derece görünür olacaktır. İnsanların damarları kesilmeyebilir, ancak insanların dayandığı devletin damarları kesilebilir.

Yapay zeka da bu duruma yeni bir katman eklemektedir; zira yapay zekanın başlı başına bir "silah" olması zorunlu değildir; ancak onu kullananların kabiliyetlerini katlayan bir güç çarpanına dönüştürebilir; dolayısıyla o, devasa miktarda veriyi analiz edebilir, zayıf noktaların keşfedilmesini hızlandırabilir, bazı süreçleri otomatikleştirebilir ve yanıltma ile sosyal mühendislik yöntemlerini geliştirebilir. Nitekim ENISA (Avrupa Birliği Siber Güvenlik Ajansı), tehdit gruplarının operasyonlarını güçlendirmek için yapay zeka araçlarını kullandığına ve kurumlar içinde ona bağımlılığın yaygınlaşmasıyla birlikte bizzat yapay zekanın da saldırı yüzeyinin bir parçası haline geldiğine işaret etmektedir. Ayrıca Ajans, önümüzdeki yıllarda siber operasyonlarda daha fazla otomasyon ve geniş ölçekli üretim görülebileceğini düşünmektedir.

Ancak belki de daha tehlikeli olan, yapay zekânın saldırı kapasitesi değil, savaşı hızlandırma kapasitesidir. Eskiden karmaşık bir operasyon hazırlamak uzun zaman ve çok sayıda insan gerektiriyordu; ancak algoritmalar bilgileri analiz etmeye, açıkları keşfetmeye, mesajlar oluşturmaya ve geniş çaplı operasyonlar yürütmeye dahil olduğunda; hedefi tespit etmekle ona vurmak arasındaki mesafe çok daha kısa bir hale gelebilmektedir.

En büyük sorun, siber bir saldırının her zaman açık bir imza taşımamasıdır; zira bir füze düştüğünde ortada fiziksel bir iz olur; fakat bir bankacılık ağı devre dışı kaldığında veya iletişim kesildiğinde, sorumlunun belirlenmesi zaman alabilir; bu süreçte organize suç, devlet destekli saldırılar, devlet dışı aktörler ve istihbarat operasyonları iç içe geçebilir. Bu da hibrit savaş veya gri bölge olarak adlandırılan şeyi oluşturur: yani doğrudan konvansiyonel savaşa varmadan aşamalı olarak siyasi, ekonomik, enformasyonel, siber ve sabotaj amaçlı bir baskı oluşturur.

NATO'nun kendisi de hibrit tehditlerini, dezenformasyon, aldatma, sabotaj ve diğer askeri olmayan yöntemleri kapsayan tehditler olarak nitelendirmekte ve son yıllarda değişen şeyin teknoloji ve küresel bağlantılılığın dayattığı hız, ölçek ve yoğunluk olduğuna işaret etmektedir. İşte burada "savaşın başlangıcı" tanımı daha da zorlaşabilir. Savaş füzeler ateşlendiğinde mi başlar, yoksa ağlara sızıldığında mı? Yoksa bir taraf rakibinin kritik altyapısını devre dışı bırakmaya

başladığında mı? Ya da operasyonların hedefi casusluk yapmak değil de diğer devleti davranışını değiştirmeye zorlamak olduğunda mı başlar?

Tankların çağı sona erdi mi? Tabii ki hayır. Burada abartıdan sakınmak gerekir. Siber savaş geleneksel savaşı ortadan kaldırmaz; aksine onun için bir zemin aşaması olabilir; zira dijital saldırılar, askeri bir saldırıdan önce gerçekleşebilir, onunla eş zamanlı olabilir veya uçaklar ve füzeler devreye girmeden önce komuta, iletişim, ulaşım ve savunma sistemlerini şaşırtmak için kullanılabilir. En dakik soru şudur: Askerî, ekonomik, siber ve enformasyon araçları tek bir savaş içinde birlikte nasıl işleyecek?

Uçak gökyüzünde, asker yerde, korsan bilgisayarın başında, finansal spekülatör işlem ekranının karşısında, dezenformasyon kampanyaları ise telefonlar üzerinden yürütülüyor olabilir; ancak onların hepsi aynı savaşın bir parçasıdır. İşte burada cephe her yerde olur. Yani kişi, bir cephede olduğunun farkında bile olmayabilir; ama geleneksel savaşta insanlar cephenin nerede olduğunu bilirler.

Görünmez savaşta cephe; telefon, banka, fabrika ve hastane de olabilir. Kişi, banka hesabına erişemeyebilir. Fabrika, dijital sistemi devre dışı kaldığında durur. Hastane, hizmetlerinin bir kısmını kaybeder. Şirket, ham maddelere ulaşamaz. Limanın sistemleri durur.

Bunlar geleneksel anlamda mutlak surette savaş sahneleri değil, ancak bir savaşın sonuçları olabilir. Bu nedenle “esneklik”, ulusal güvenliğin temel bir parçası haline gelmiştir; zira NATO, siber saldırılar ve hibrit tehditlerle mücadele de dahil olmak üzere ülkelerin dayanıklılık kapasitesini ulaşım, iletişim, enerji, gıda, su, ilaç, kamu yönetimi ve bilgi akışının korunmasıyla ilişkilendirmektedir.

Tedarik zincirleri; daha önce istisnai olarak görülen savaş araçlarından bir kısmı, artık devletler arasındaki rekabette fiilen yer almaktadır. Avrupa kurumları binlerce siber olayı belgelemiş olup raporlar, devletlerle bağlantılı aktörlerin faaliyetlerinin sürdüğüne ve bazı kötü niyetli operasyonlarda yapay zekâ kullanımının arttığına işaret etmektedir.

Eğer savaşın başladığını söylemek için tankların gelmesini bekliyorsak, savaşın uzun zaman önce başladığını keşfedebiliriz. Eğer her siber saldırıyı bir savaş olarak kabul edersek; bu kez de suç, casusluk, sabotaj ve askeri çatışmanın arasını karıştırmış oluruz. Bu nedenle önümüzdeki aşama çok daha dakik bir ölçüte ihtiyaç duymaktadır: Yani devlet, rakibini siyasi ve stratejik olarak zorlamak amacıyla rekabet, caydırıcılık ve gizli operasyonlardan düzenli güç kullanımına ne zaman geçer?

Savaş, sunucu, ağ, deniz tabanındaki kablo, uydu, bankacılık sistemi ya da tedarik zinciri gibi kimsenin dikkat etmediği bir yerden de başlayabilir. Gelecekteki savaşta ilk soru şu olmayabilir: Bizi kim bombaladı? Dolayısıyla son derecede birbirine bağlı bir dünyada, savaşın ülkenize girmesi için artık sınırları aşmasına bile gerek kalmayabilir.

Hizb-ut Tahrir Merkezi Medya Ofisi İçin Yazan
Nebil Abdulkerim