Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi

YAZILIM SEKTÖRÜNDEKİ ŞİRKETLERİN YABANCI ŞİRKETLERE SATILMASININ İSTİHBARAT VE SİBER GÜVENLİĞE ETKİSİ

HAKTAN AKDAĞ

GİRİŞ

Bu makalede yazılım sektöründeki ekosistemi, ve ekosistemin getirilerinden daha değerli çıktısı olan verinin analizi sonucunda hangi değerlerin elde edilebileceğine dikkat çekmek amaçlanmıştır. Günümüzde konvansiyonel savaş stratejilerinin de ötesine geçen enformasyon savaşları kapsamında değerlendirildiğinde bir "bilgi > (büyüktür) bir mermi" çıkarımı yapmaktadır.

İstihbarat kavramı özellikle stratejik üstünlük sağlayabilmek için her ne kadar ön planda tutulsa da İstihbaratın ham maddesi olan bilginin ve analiz edilebilir kazanılmış bilginin değeri artık çok daha değerli bir hal almıştır. Geçmişte savaş stratejileri oluşturulurken ülke içi öz kaynakların mevcut durumu değerlendirilir ve ona göre stratejiler oluşturulurdu, Günümüzde karşı ülkelerin de ülke içi iç ve dış kaynaklarını kontrol edebilen güçler hasım ve hasım olması muhtemel ülkelere karşı önlemler veya adımlar atabilmek için mevcut iç ekosistemine hâkim olmak zorundalar. Finansal güç her yönden strateji belirlerken üstünlük sağlayacağından karşı ülkenin finansal durumunu biliyor olmak ve mevcut ekonomik durumu hakkında yorum yapabiliyor olmak çok önemli bir istihbarat aracı haline dönüşmektedir. Ülkeler yerli ve milli silah teknolojilerini üretirken askeri stratejik üstünlük sağlamayı hedefledikleri için tüm yatırımlarını öncelikli olarak bu alana yöneltseler de, özellikle ülke içi ekosistemin yönetilmesini sağlayan endüstriyel yazılımların da yerli ve milli olması için stratejik adımlar atılması gerekmektedir. Bugün dünyanın önde gelen siber güvenlik yazılımları veya endüstriyel otomasyon yazılımlarının neredeyse tamamı ABD, İsrail, Almanya tekelinde piyasa hakimiyetini korumaktadır. Rusya sadece bu yüzden bile yerli ERP sistemlerini geliştirmekte ve iç piyasada mevcut yerli sistemin kullanılmasını yaygınlaştırmıştır. Aynı şekilde, eposta servisleri, sosyal medya ve çeşitli güvenlik yazılımları konusunda da ülke içi kaynaklar ile yaratılmış ürünleri dünya piyasasına açmaya devam etmektedir. Altyapısı kendi kontrolünde olan sosyal medya platformlarının yönetilmesi iç iletişimde üstünlük sağlamakta, hatta farklı ülkelerde çeşitli enformasyon savaşları yürütmek için araç şeklinde kullanılmaktadır. Rusya için (Yandex , Telegram , VK) bunlara örnektir.

Yazılım tarihine bakıldığında geçmişten günümüze kaynak kodlarının fikri sınai mülkiyet hakkı kapsamında değerlendirildiği, fakat bir fikir patenti kapsamında değerlendirilmediği görülmektedir. Çünkü belirli formül veya yöntemler doğrultusunda bir amaç için geliştirilen yazılımların kaynak kodlarının mı değerli olduğu, yoksa çözüm sunulan fikrin mi değerli olduğu zaman zaman tartışılmaktadır. Bu çalışmada dikkat çekilmek istenen konulardan biri de yazılımın kodları veya amaçlarından ziyade ortaya çıkardığı verinin de değerli olması, faaliyette bulunduğu mevcut ekosistemin paydaşlarından biri olması ve ne kadar değer yarattığından ziyade ne kadar değerli data yarattığıyla ilgilenilmesidir.

Diğer yandan siber güvenlik kavramı, siber uzayın günlük yaşantımıza entegre olması ve bu ortamda ortaya çıkan güvenlik endişeleriyle bağlantılıdır. Daha önce sıkça ele alınan siber güvenlik, 2009'da Amerikan Başkanı Barack Obama'nın Amerikan halkını siber güvenliğin önemine dikkat çekmeye, ulusal güvenliği sağlamak için uygun etkinlikler ve eğitimler düzenlemeye davet etmesiyle önemli bir popülerlik kazanmıştır (Alp, 2018, s. 36). Siber güvenlik, siber ortamdaki verilerin kullanım, dolaşım ve depolama aşamalarında korunmasını, bu korumayı hedefleyen politika ve prosedürleri, güvenliği temin edecek her türlü teknolojiyi içermektedir. Kuruluşların ve bireylerin siber ortamda bulunan varlıklarını koruma amacını taşıyan siber güvenlik, sürekli bir mücadele gerektirir. Bu mücadele, siber ortam tehditlerine karşı güncel teknolojik gelişmelerin izlenmesini, politika ve prosedürlerin düzenli olarak gözden geçirilmesini ve uygulanmasını içermektedir (Arslan, 2021, s. 18).

İstihbarat, bilgi toplama, analiz etme ve çeşitli tehditlere karşı korunma amacıyla faaliyet gösteren stratejik bir disiplindir. İstihbarat faaliyetleri genellikle özel ve gizli olarak sürdürülür, çünkü bilgiye erişim ve bu bilginin doğru bir şekilde değerlendirilmesi, ulusal güvenlik açısından kritik öneme sahiptir. İstihbarat teşkilatları teknolojik gelişmeleri takip ederek, insan kaynaklarından elde edilen bilgileri analiz ederek ve çeşitli operasyonlar

düzenleyerek güvenlik açısından kritik öneme sahip bilgileri elde etmeye çalışırlar. Sadece devletlerarasında değil, aynı zamanda uluslararası örgütler, terör grupları ve diğer aktörler arasında da istihbarat faaliyetleri gerçekleşebilir. Bu nedenle istihbarat çalışmaları karmaşık bir küresel arenada gerçekleşen dinamik değişimlere hızla uyum sağlama becerisini gerektirir.

Bu makalenin temel araştırma konusu yerel teknoloji firmalarının ülke ekonomisi üzerindeki etkisine dayanarak finansal ve operasyonel faaliyetlerinin ekonomik espiyonaj çerçevesinde korunması konusuna dikkat çekmektir. Bu konunun siber güvenlik kapsamında değerlendirilmesi uluslararası arenada dünya ülkelerinin finansal espiyonaj faaliyetlerinin önlenmesi için önemlidir. Büyük ülkeler finansal ve ekonomik yaptırımlarını diğer ülkeleri kontrol ettikleri şirketler vasıtasıyla gerçekleştirirler. Uluslararası para piyasalarında bile zaman zaman bunun yansımalarını görürüz. Bunun en basit örneği borsa manipülasyonu ile yaptırım uygulamak istedikleri ülkelere çeşitli operasyonların yapıldığına tanık olmaktayız, bu durumun daha kapsamlı versiyonu özellikle finans ve teknoloji şirketleri üzerinden yapılabilecek potansiyel operasyonların önceden ön görülmesi için diğer büyük dünya ülkeleri çeşitli önlemlerin aldıklarını görmekteyiz.

Bugün kurumsal ve ekonomik casusluk yasasının ABD 1996 yılında yürürlüğe girmesinin sebeplerinden biri de aslında uluslararası alanda faaliyet gösteren ekonomik tetikçilerin ülkemiz içindeki faaliyetlerini önlemek adına söz konusu yasaya benzer yaptırımlar için yasalar çıkarttığını görüyoruz (Yücelik, 2015, s.3).

Devlet sırlarının korunması için casusluk faaliyetlerinin önlenmesi için sadece devletin siyasal ve idari faaliyetleri kapsamında önlemler alınması yeterli değildir, devletin vatandaşını koruması ile ilgili tüm önlemlerin alınması doğrultusunda işleyişin yapılandırılması gerekliliği olarak ifade edilebilir (Köken ve Gül, 2020, s.4).

1. KAVRAMSAL ÇERÇEVE

Şekil 1 de gösterildiği gibi bir yazılım şirketinin yaratmış olduğu ekosistem kaynağından birçok gelir modeli elde edilebilmektedir. Hatta lisans veya yaratılan ekosistem gelirinin olmadığı modellere de sektör zaman zaman şahitlik eder.

Danışmanlık geliri; sektörel bilgi birikimi gerektirmektedir. Özellikle makine üretimi konusunda uzmanlaşmış uygulama danışmanları yetişir ve söz konusu iş süreçlerini benzer sektörlere uygulayabilecek uzmanlar oluşturur.

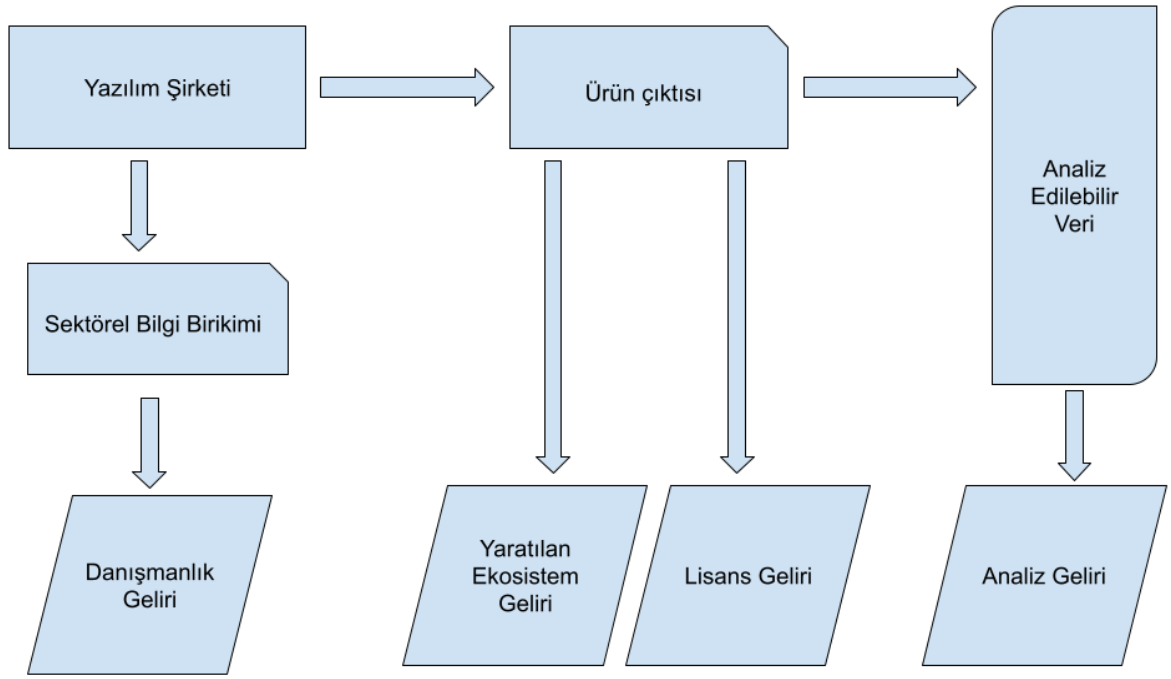
Yaratılan ekosistem geliri: Bir sistemin satışı, kurulması ve pazarlanması sürecinde bir çok firma veya kişi bu söz konusu ekosistemden faydalanabilir. Dijital dönüşüm uzmanları, yazılım satış uzmanları ve iş geliştirmeciler bu ekosistem içinden fayda sağlayan ve ortaya çıkanlardır.

Lisans geliri: Bu gelir üzerinden belirlenen oranlarla kar marjları dağıtılarak gelir modeli oluşturulur. Yazılım firmaları ürün ve hizmetlerini bölgesel olarak satıp pazarlayacak bayi, distribütör veya kanal yapıları kurmak için yatırımlar yaparlar. Bölgesel yaygınlaştırmayı artırmak için ekosistem içindeki paydaşlarına ciddi kar oranları paylaşırlar.

Analiz geliri: Tam olarak bu makalenin konusunu oluşturmakla birlikte, gizli ve büyük pastanın oluşturulması amaçlanmıştır. Bu gelir modeli ekosistemin alt kısmıyla paylaşılmaz ve etik dışı bir gelir modeli olduğundan genellikle gizliliğini korur. Zaman zaman kamuoyuna

yansıyan dava veya ifşalar ile ortaya çıksa da aslında herkesin bildiği fakat kimsenin ispatlayamadığı bir gerçeklik olarak ekosistem içindeki en büyük paydır.

Şekil 1. Yazılım Ekosistemi (Kaynak: Yazar)



Örneklendirmek gerekirse, Yazılan uygulamalar ücretsiz veya lisanslama konusunda çok katı olmayan politikalar izleyerek sektörde ürünü yaygınlaştırma stratejileri uygular. Kullanıcılar uygulamayı lisanssız da kullansa yazılım üreticisi belli bir süre veya stratejisine göre uygulamanın kullanımını durdurmaz. Özellikle sistem tasarlayıcıları sistemin lisanssız bir şekilde kullanılmamasını sağlayabilecekken, söz konusu yaygınlaştırma politikasından kaynaklı sistem içine arka kapı yerleştirerek yine resmi olmayan yollarla ürünlerinin lisanssız kullanımına müsaade ederler. Burada ürün yaygınlaştıktan sonra kullanıcı verilerini ve verilere ait çıktıların analiz geliri ticarileştirebilirler. Söz konusu makalede buradaki analiz geliri yaratabilecek çıktıların gelirden ziyade daha kritik zararlara yol açabilecek nitelikte stratejik verilerin korunması gerektiği önemi vurgulanmaya çalışılmaktadır. Özellikle sistem tasarlayıcılar, sistemlerin yan veya ana kazanım yöntemlerinden çok nihai çıktı olan pastanın büyük dilimini kendilerine ayırmak üzere ekosistem oluştururlar. “Bir ürüne ücret ödemediyseniz, ücret sizsiniz” anonim söyleminden yola çıkarak yaratılan bu sosyolojik algı sayesinde bırakılan dijital izler takip edilerek kullanıcı alışkanlıklarını takip eden sistem kurucuların daha da ileriye giderek kullanıcı ihtiyaçlarını analiz ettiği günümüzde, kurumsal işletmelerin hareket alışkanlıklarına göre ticari faaliyetlerini analiz etmeleri kaçınılmazdır. Bu durum makro ekonomik ölçüde incelendiğinde ülkenin stratejik adımlarını ekonomik düzeyde irdeleyebilecek şekilde bir çıkarım oluşturacaktır.

1.1. Yazılım

1950’lerin ortalarında bilgisayarların ticari kullanımının başlamasıyla birlikte, tüm yazılım sistemleri genellikle şirket içinde geliştirilmekteydi. O dönemde yazılım endüstrisi henüz tam

olarak gelişmemişti. Yazılım endüstrisinin ilerlemesiyle birlikte, birçok kuruluş yazılım ihtiyaçlarını özel yazılım sağlayıcılara dışarıdan temin etmeye başladı. Ancak çoğu yazılım ürünü genellikle özel olarak her kuruluş için geliştirilmekteydi. Diğer bir deyişle, standartlaşmış yazılım ürünleri çok sınırlıydı. Bu sebeple, yazılım endüstrisinde bir sonraki adım, yazılım üreticilerinin bir kez geliştirdikleri yazılımı birden fazla müşteriye satma yoluna gitmeleri oldu. Bu yaklaşım, üreticilere kendi tescilli yazılımlarını geliştirerek ölçek ekonomilerinden faydalanma imkânı tanıdı (İslah, 2023, s. 64).

Yazılım olmaksızın, birçok bilgisayar işlevsiz hale gelir ve sadece bir cihazdan ibaret kalır. Örneğin, bir web tarayıcısı, kullanıcıların internete erişimini mümkün kılan bir yazılım uygulamasıdır. İnternete erişim sağlayan bu yazılım olmadan, web tarayıcısını kullanmak mümkün olmaz. Bir işletim sistemi olarak görev yapan yazılım programı, diğer uygulamalarla etkileşimde bulunmak ve bir bilgisayar veya mobil cihazdaki donanımla iletişim kurmak için bir ara yüz sunmaktadır (Tang vd., 2010, s. 616).

Yazılım, düşük maliyetli üretimi ve yüksek değerli ürünleriyle gelişmekte olan ülkeler için avantajlar sağlayan yaratıcı bir sektördür. Bilgi ekonomisinin alt sektörü olarak, küresel rekabetçi piyasada doğrudan veya dolaylı olarak teknoloji tabanlı tüm sektörlere entegre edilebilen bir yapı sunmaktadır (Köse, 2019, s. 73).

Yazılım genel olarak, belirli bir hedefi gerçekleştirmek ve elektronik bir cihazda işlevleri yerine getirmek amacıyla kullanılan bir programlama dilinde yazılmış bir dizi bilgisayar talimatıdır. Bu talimatlar, bir derleyici aracılığıyla merkezi işlem biriminin işleyebileceği bir nesne koduna dönüştürülen kaynak kodunu oluşturur. Başka bir ifadeyle, yazılım, verilen verileri yönetmek için bilgi ve programlar kullanılarak temsil edilir. Bu bağlamda, söz konusu bilgi, bir veya daha fazla program veya bir veya daha fazla veri veya her ikisinin bir kombinasyonu aracılığıyla ifade edilebilir (Moro-Visconti, 2020, s. 287).

1.2. Yazılım Sektörü

Yazılım sektörü, hızla değişen teknolojik peyzajda belirgin bir rol oynayan dinamik bir endüstridir. Günümüzde, bu sektör sadece bilgisayarlarla sınırlı kalmayıp mobil cihazlar, bulut bilişim, yapay zekâ, büyük veri ve diğer birçok alanı içine alarak geniş bir yelpazeye yayılmış durumdadır. Yazılım sektörü aynı zamanda endüstri sınırlarını aşan bir etkiye sahiptir. Sağlık, finans, eğitim ve üretim gibi birçok sektördeki kuruluşlar, özel yazılım çözümleriyle iş süreçlerini optimize etmeye çalışmaktadır. Bu da sektörün sadece bir destekleyici değil, aynı zamanda bir dönüştürücü güç olarak konumlanmasına neden olmaktadır.

UNCTAD (2012) Yazılım Raporu'na göre, yazılım sektörü iki ana kategoride faaliyet göstermektedir. Bunlar: Yazılım Ürünleri ve Yazılım Hizmetleridir. Yazılım ürünleri, tüm işlevsel gereksinimleri karşılayarak yazılıma ait temel özellikleri sunar. Diğer yandan yazılım hizmetleri ise üretilen yazılımların bilgi ve iletişim teknolojileri aracılığıyla sürdürülebilirliğini sağlamak ve yeni gelişmeler için destek sağlamak amacıyla hizmet verir.

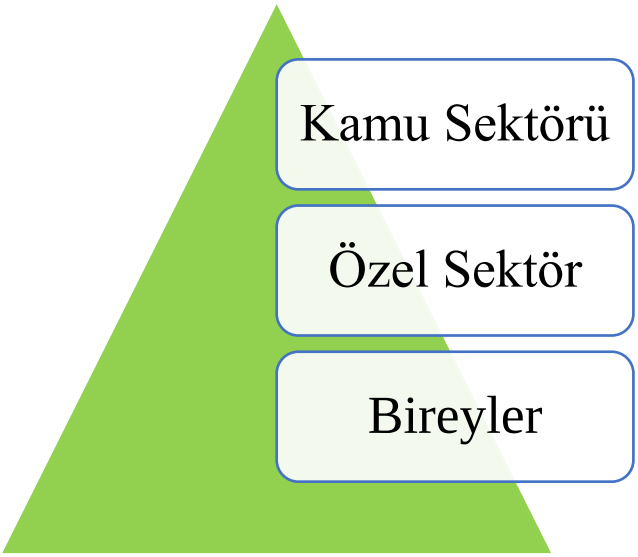
Yazılım sektörü, sadece oluşturduğu dış ticaret hacmiyle değil, aynı zamanda farklı sektörlerde ve kamuda olumlu bir etki yaratmaktadır. Güçlü yazılım şirketleri, sadece ürünleri aracılığıyla diğer şirketlerin dönüşümüne katkıda bulunmakla kalmayıp aynı zamanda yetenekli yazılım geliştiricileri ile sektör ekosistemini desteklemektedir. Ayrıca, sağlık,

savunma, eğitim gibi kamu kurumlarının dönüşümleri de yazılım tabanlı çözümler sayesinde gerçekleştirilmektedir (Deloitte, 2021).

1.3. Siber Güvenlik

Şu anda yaşadığımız dünyada teknoloji, sadece insanların günlük yaşamlarını değil, iş dünyasından kamusal alanlara kadar geniş bir yelpazede hayatımıza nüfuz etmiştir. Bir topluluğun siber uzayını temsil eden bireyler, kişisel ve kritik verilerini özel ve kamusal sektörlerde kullandıkları teknolojiler aracılığıyla siber uzaya aktarmaktadır. Teknolojinin ilerlemesi ve hayatımıza daha fazla entegre olmasıyla birlikte, milyonlarca liralık milli güvenliği ilgilendiren kritik veriler, dünya siber uzayında savunmasız bir şekilde dolaşmaktadır ve çeşitli siber saldırılara açık hale gelmiştir (Usom, 2014, s. 2).

Şekil 2. Siber Uzayın Bileşenleri (Kaynak: Usom, 2014, s.3)



Yukarıda bahsedilen önemli süreçlere ek olarak, bireylerin kişisel bilgilerini siber uzayda depolamaları, kullandığımız teknolojilerin istikrarlı, güvenli, güvenilir ve esnek bir yapıda olmasını zorunlu kılar. Çünkü günümüzde, siber suçlular ve teröristler, bilgisayarları, bilgisayar ağlarını, mobil cihazları ve akıllı cihazları amaçlarına ulaşmak için giderek artan bir şekilde kullanmaktadır. Siber suçlular tarafından gerçekleştirilen kişisel veri sızıntıları ve kötü niyetli kullanımlar, kritik süreçlerin engellenmesine veya yok edilmesine, ekonomiye ciddi maliyetlere neden olan saldırılara yol açabilir ve milli sırların ele geçirilmesi veya ifşa edilmesi gibi bir dizi siber tehdidi beraberinde getirebilir. Bahsedilen birçok siber saldırının önlenmesi, yukarıda Şekil 1'de belirtilen siber uzay bileşenlerinin korunmasını sağlamak için alınacak önlemlere dayanmaktadır (Usom, 2014, s. 3).

Siber güvenlik, bilgisayar ağlarını, donanımları ve kıymetli verileri yetkisiz erişimlerden veya suç amaçlı kullanımlardan korumak için yapılan çalışmaları içerir; bu çalışmalar aynı zamanda bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini güvence altına almayı amaçlar (Schatz vd., 2017, s. 60). Siber alanda faaliyet gösteren bilgisayar ağları, sunucular, mobil cihazlar, elektronik sistemler veya veri ağları ve bu sistemlerde çalışan yazılımları siber tehditlere karşı korumak için alınan önlemleri kapsar. Bilgisayar sistemlerine yönelik güvenlik endişeleri, internet ve kablosuz ağ standartları gibi Bluetooth ve Wi-Fi ile akıllı

telefonlar, televizyonlar ve çeşitli cihazları içeren Nesnelerin İnternet'inin büyümesiyle birlikte sürekli olarak artmaktadır. Siber güvenlik, hem politik kullanım hem de teknoloji karmaşıklığı nedeniyle çağdaş dünyadaki önemli zorluklardan biridir (Kianpour, 2021)

1.4. Sektörün İstihbarat Kavramındaki Yeri

Tanımlanan istihbarat kavramları temel anlamda devlet ve uluslararası güvenlik stratejileri ile bağdaşsa da özellikle istihbarat kavramının özelleşmesi son yıllarda oldukça yaygınlaşmıştır. Özel askeri şirketlerin artması ve özel istihbarat şirketleri vasıtasıyla ülkeler örtülü operasyonlar yürütmekte bilgi ve belge tedariği için her türlü kurum veya özel şirkete haber elemanı devşirme çalışmaları yürütülmektedir. Özellikle son yıllarda örtülü operasyon yürütmek üzere kurgulanmış, finansal yapısı ve teknolojik altyapısı ülkelerin istihbarat servisleri tarafından desteklenen birçok yazılım şirketi kurulduğunu ve yönetildiğini zaten biliyoruz. Fakat resmi bir şekilde tam olarak açıklanmadığı için bu tespitler komplo teorisi gibi gözükebiliyor. Sonuç olarak bu yöntemin başarılı olduğunu söyleyebiliriz. Hatta bu makale ile bu teoriyi biraz daha genişleterek özel istihbarat şirketlerinin bizim gibi ülkelere teknoloji satarak veya bizim teknolojilerimizi satın alarak ne derece kazanımlar elde etmeye çalıştıklarından bahsetmeye çalışacağım. Özellikle Avrupa ve ABD radikal terör örgütü faaliyetlerini engellemek için istihbarat servisleri dijital ortamlarda veya sosyal medya platformlarında sahte terör hesapları yaratıp teröre destek verebilecek potansiyel kullanıcıları tespit etmekte ustalaştılar. Dark web (deep web) in içinde her ne kadar illegal yöntemler ve illegal iş bilgileri bulunsa da bunlardan birçoğu özel istihbarat servisleri tarafından yönetilen yöntemlerle doludur. Zaten illegal bir yönteme giren bir kullanıcı, illegal örgütler ile temas kurduğunda hangi servis veya örgütün amaçları doğrultusunda yönlendirileceği bilemeyeceğinden hedeflediği bilgi ve belgeyi elde etmek adına kendisi ile ilgili çok fazla dijital iz bırakacaktır. Özel filtreleme yazılımları veya güvenlik yazılımları kullanmıyorsa o derece güvensiz bir ortamdan güvenli bir şekilde çıkabilmesi neredeyse mümkün olmayacaktır. Dolayısıyla söz konusu siber istihbarat çalışmaları çok yoğun bir biçimde dark (deep) web de devam ederken, legal yöntemler ile elde edilebilecek kazanımları da yadsımamak gerekmektedir.

Bu çalışmanın temel argümanı, bir ülkede yazılım sektörünün yabancı şirketlerin kontrolüne/tekeline geçmesi finansal ve teknolojik açılardan istihbarat zafiyetine neden olabilecektir. Bu çalışma yukarıda belirtilen temel varsayım çerçevesinde öncelikle yazılım kavramının genel hatlarını, yazılım ile siber güvenlik arasındaki ilişkiyi, siber güvenliğin istihbarat alanındaki yeri ve önemini aktardıktan sonra Fintech'in bu süreçteki yerini incelemektedir. Böylece makale, Fintech'i örnek olgu olarak değerlendirerek çalışmanın ana konusu olan yazılım-istihbarat zafiyeti ilişkisini şirket değerlemesi, bulut bilişimi, yazılım sistemleri, iş yazılımının geleceği gibi boyutlar çerçevesinde ele almayı ve yukarıda belirtilen argümanı desteklemeye çalışmayı hedeflemektedir.

İstihbarat kavramı içindeki bu makalenin konusu olan argümanları özetlemek gerekirse, yasal yollarla elde edilen bilgileri yasal olmayan yollarla yurt dışına çıkarmanın önüne engel koyabilmek için veriyi kaçıranları yakalamak yerine veriyi kaçıranları verinin olduğu yere sokmamak gerektiğini düşünüyorum. Paravan şirketler ile ülkemizdeki finansal ve üretim planlama süreçlerini yöneten yazılım sistemlerinin ve söz konusu sistemlerin ürettiği verilerin tamamının korunması teknik olarak mümkün olmasa bile, belli bir kontrol çerçevesinde korumak için farkındalığı arttırmak gerekmektedir. Bugün verinin petrolden daha değerli

olduğunun tespitini yaparken, bir petrol yatağını korumak için devletin aldığı önlemlerin bir kısmını da kıymetli veri üretebilecek yazılım sistemlerinin stratejik konumlanması sırasında çeşitli denetimler yapmak gerekmektedir.

Sanayinin gelişmesi, dijital dönüşümün yaygınlaşması, süreçlerin iyileştirilmesi için devlet destekleri sağlanmakta, bu destekler ile büyütülen ekosistemin yarattığı veriyi analiz etsinler diye uluslararası hasım ve hasım olması muhtemel ülkelere göndermemek adına ticari yatırımcı faaliyetlerini de irdelemek gerekmektedir.

Potansiyel stratejik üstünlük sağlamaya çalışan ülkelerin ülkemiz içindeki taşeronlarına değerli verimizi analiz etmeleri almaları onlara çok ucuza mal olduğundan bizler için ilerde çok pahalıya mal olacak süreçler yaşamamıza neden olacaktır.

1.5. Fintech Nedir?

Açık bankacılık kavramının ortaya çıkmasından sonra özellikle bankaların görev ve sorumluluklarına benzer bazı faaliyetleri yerine getirebilmek ve söz konusu faaliyetleri özel şirket manevrasıyla ortaya koyabilmek için finans teknolojileri ile ilgili şirketler kuruldu, Dünyada özellikle ödeme sistemlerini ve para tahsilatı ile ilgili tüm süreçleri kolaylaştıran uygulamalar bir anda geliştirildi. Özellikle kripto paranın yaygınlaşması ve devletlerin kripto parayı yasal bir değer olarak kabul etmemesinden kaynaklı, söz konusu ödeme alma araçları kripto para ile ödeme alınabildiği için son kullanıcı ve özel şirketler tarafından tercih edildi ve yaygınlaştı (Keyofchange, 2022a).

Fintech kavramının yaygınlaşması ve ilerlemesi için siber güvenlik kavramlarının geliştirilmesi ve iyileştirilmesi gerekmektedir. Özellikle para bilgisinin taşınması, entegre edilmesi verinin manipüle edilmemesi ile ilgili çok önemlidir. Buradaki siber güvenlik kavramı sadece siber güvenlik sistemlerinin veya donanımlarının değil, yazılım teknolojileri ile ilgili geliştirilen kodların ve uygulamaların da güvenlik prosedürlerine uygun bir biçimde yapılması gerekmektedir. Ayrıca bir siber protokol oluşturulmalı ve siber istihbarat ile ilgili bu prosedürlerin devletin çeşitli kurum ve kuruluşları tarafından denetlenmesi gerekmektedir.

Kurulabilecek çeşitli siber güvenlik birimlerinin oluşturacağı protokoller çerçevesinde belge veya sertifika yöntemleri ile süreçler bir standarda bağlanabilecektir. Özellikle finansal süreçlerin olduğu bankalardaki siber ekiplerin prosedürleri kadar büyük olmasa da bir prosedür ve standardın var olması ortaya çıkabilecek saldırıların bir nebze de olsa önüne geçebilecektir Keyofchange, 2019).

Fintech teknolojinin finans ve ekonomik süreçlerin hızlanması, şirketlerin ticari faaliyetlerini hızlandırmak için birçok avantaja sahiptir.

Dijitalleşen dünyada teknolojiyi takip eden kurumlar finansal teknolojileri de takip etmek durumundadır. Fintech dijitalleşmesini sağlayan kurumlar tüm finansal süreçlerinde otomatik iş süreçleri oluşturulabilir ve tüm süreçler hızlandırılabilir, kolay ulaşılabilirdir ve kurulum uyarlaması hızlıdır, kullanıcı deneyimleri sürekli olarak iyileştirilir, son kullanıcı ve kurumlar için avantajlı – rekabetçi fiyatlara sahiptir. Fakat verilerin devletin denetlediği bir bankanın elinde değil de henüz denetlenmeyen bir şirketin elinde olması, güvenlik süreçlerinin şirketin sorumluluğunda olması ve her an ticari veri hareketlerinizin çalınma riski, finansal büyüklüğünüzün başka bir şirket tarafından bilinebiliyor ve analiz edilebiliyor olması, nakit akış hızınızın sizin dışınızda biri veya birileri tarafından analiz edilebiliyor olması, finansal (Özel) kredi kuruluşlarına bilgilerinizin analiz edilebilmesi için verilmesi veya verilebilecek olması finansal istihbarat konusunda bir zafiyet niteliğindedir.

2. ÇALIŞMA İLE İLGİLİ GÖRÜŞ VE DEĞERLENDİRMELER

2.1. Şirket Değerleme Mekanizmalarının Yenilenmesi

Bir şirketin değerlemesini yapabilmek için iktisatçıların veya finansçıların çeşitli formül ve yöntemleri mevcuttur. Fakat çok ciddi mal varlığı olan, nakit akışı oldukça fazla olan şirketlere nazaran, 2-3 kişilik bir "startup" olan yazılım şirketlerinin standart kurallara göre bakıldığında aşırı değerli çıkması, mevcut formül ve hesaplamaların yanı sıra, artık işin içine farklı parametrelerin de girdiğinin göstergesidir. Burada dikkat edilmesi gereken konu teknik olarak teknolojik anlamda yetenekli bir ürünün olduğundan fazla değerli gösterilmesinin altında yatan nedenlerin iyi irdelenmesi gerektiğidir. Özellikle ürünün konumlandığı alanın neye göre ve kime göre değerli olabileceği önemli bir noktadır. Bilgi ve belge toplayabilecek, analiz yapabilecek bir konumda bulunan her yazılım bulunduğu konumdan dolayı olduğundan fazla değer görmektedir. Savunma sanayinde bulunan güvenlik ürünlerindeki yazılımlar kadar değil gibi görünen ticari sistemler, özellikle iç stratejileri izleyebilmek için çok kullanışlı sistemler olduğundan dış istihbarat kurumlarının veya istihbarat şirketlerinin desteklediği şirketlere satılması bir ulusal güvenlik meselesi haline gelmiştir (Fastcompany, 2023).

2022 yılında ekosistem üzerinden dönen para sayesinde şirketlerin büyüme oranları yüzde 65-70 iken 2023 yılında internet şirketlerinin büyüme oranları yüzde 100-125 oranındadır. Bu oranlar öyle bir anda yeni kurulan bir şirketin çok büyük oranda büyümesi oranı değil, aksine 75 milyar TL gibi bir parayı kendi ekosistemi içinde çevirebilecek nitelikteki büyük şirketlerin oranlarıdır. Ülke ekonomisinin büyük bir kısmını domine eden söz konusu bu internet şirketleri genellikle e-bahis(yasal), e-ticaret, yazılım, oyun vb. kategorilerdeki sistemlerdir (Fastcompany, 2023).

2.2. Bulut Bilişim

Bilgilerin bulutta saklanması kavramını çoğu kişinin aşina olduğu bir kavramdır. Teknolojinin ve internet teknolojilerinin gelişmesiyle, bulut bilişim kavramı son kullanıcının hayatına olabildiğince girmiş durumdadır. Verilerin local sunuculardan ziyade kiralanan veya hizmet olarak satın alınabilen ya da yeterli teknik altyapı varsa kendi bulut bilişim altyapısını kurmayı amaçlayan kurum ve kuruluşlar, teknolojilerini ve uygulamalarını bulut bilişim altyapısına ya taşındılar ya da kısa süre içinde taşımak durumundalar. Özellikle internet üzerinde yapılan araştırmalara göre 2025 yılına kadar bulutta 100 zerabayttan fazla veri depolanmış olacaktır (Map, 2022).

Özellikle ABD'li bilişim şirketleri, yaptıkları sunucu ve internet altyapısı yatırımlarıyla dünyadaki bulut bilişim altyapısının neredeyse yarısına sahip ve tüm pazarı domine edebilecek güçtedir. Kamu kurum ve kuruluşların yerli yazılım ile ilgili yaptığı sürekli bildirilere rağmen kurumların verilerini ABD'li şirketlerin kurduğu altyapılarda depolanması da ayrıca bir güvenlik problemi olarak karşımıza çıkmaktadır. Kamu kurumlarındaki verilerin yurt dışı kaynaklı servis sağlayıcılarda saklanmaması ile ilgili gerekli çağrıları yapmakta ve yerli servis sağlayıcılar ile ilgili prosedürleri uygulamakta fakat özellikle özel kurum ve kuruluşların genellikle fiyat avantajından ve performanstan kaynaklı yurt dışı hizmet veren servis sağlayıcıları tercih etmektedirler. Son kullanıcı yani kişisel kullanım için kullanılan bulut bilişim altyapısının büyüklüğünden bahsetmeye bu makale özelinde bahsetmeye gerek duymuyorum, fakat bugün dünya çapında kurumsal verilerin neredeyse yarısı bulutta tutulmaktadır.

Bulut sistemlerinde tutulan verilerin güvenliğini bulut bilişim altyapısını sağlayan servis sağlayıcılar tarafından sağlansa da oluşabilecek bir güvenlik açığının sorumluluğunu üstlenen bir yapı olmadığı gibi, söz konusu zararlarla ilgili suçlanabilecek dünya çapında bir kurum kuruluş veya yaptırım olmadığını da belirtmek isterim. Güvenlik protokollerine uyulup uyulmadığını kontrol edebilecek mekanizmaların da otorite olarak kabul edilmediği düşünüldüğünde büyük dünya ülkelerinin kendi sosyal ağları veya kendilerine ait bilişim servis sağlayıcılarına neden bu kadar büyük yatırımlar yaptığını da anlamak gerekmektedir.

Özellikle Rusya ve Çin'in, ABD'ye ait sistemlere alternatif kendi sistemlerini yarattıklarını gözlemlemekteyiz, bunun sebebi ulusal anlamda bir ambargo, savaş veya çeşitli saldırı faaliyetleri olması durumunda söz konusu servislerin düşman ülkeler tarafından kapatılabileceğini ve içeride ulusal düzeyde sorunların büyüyebileceği öngörülmektedir. Bu yüzden ülkemizdeki büyük yazılım şirketlerinin, kendi bulut sistemi altyapısını kurmalarını, kurmak için yatırımlar yapmalarını ve yapılan yatırımlar sonucu oluşan altyapıların yine kobilere hizmet ve servis olarak satılmasının sağlanması gerekmektedir. Bu konuda yapılan yatırımların çeşitli vergi avantajlarından faydalanılarak yapılması yönünde devletin de elini taşın altına koyması gerekmektedir.

2.3. Verinin Değeri

Verinin önemini vurgulamak için ortaya koyulabilecek en açık ölçüt, verinin katkı sağladığı çalışmalardaki değeridir (Doğan ve Arslantekin, 2016, s. 19). Verinin değeri ve potansiyelini tam olarak ortaya koymak için, işletmelerin ürettikleri ve karşılaştıkları verilerle ilişkilerinin seviyesini incelemek faydalı olabilir (Atan, 2016: 138). En değerli varlığınızı yani verinizi bir başkasına emanet eder misiniz? Bulut bilişim altyapısına geçtiğinizde bu sorunun cevabı evet

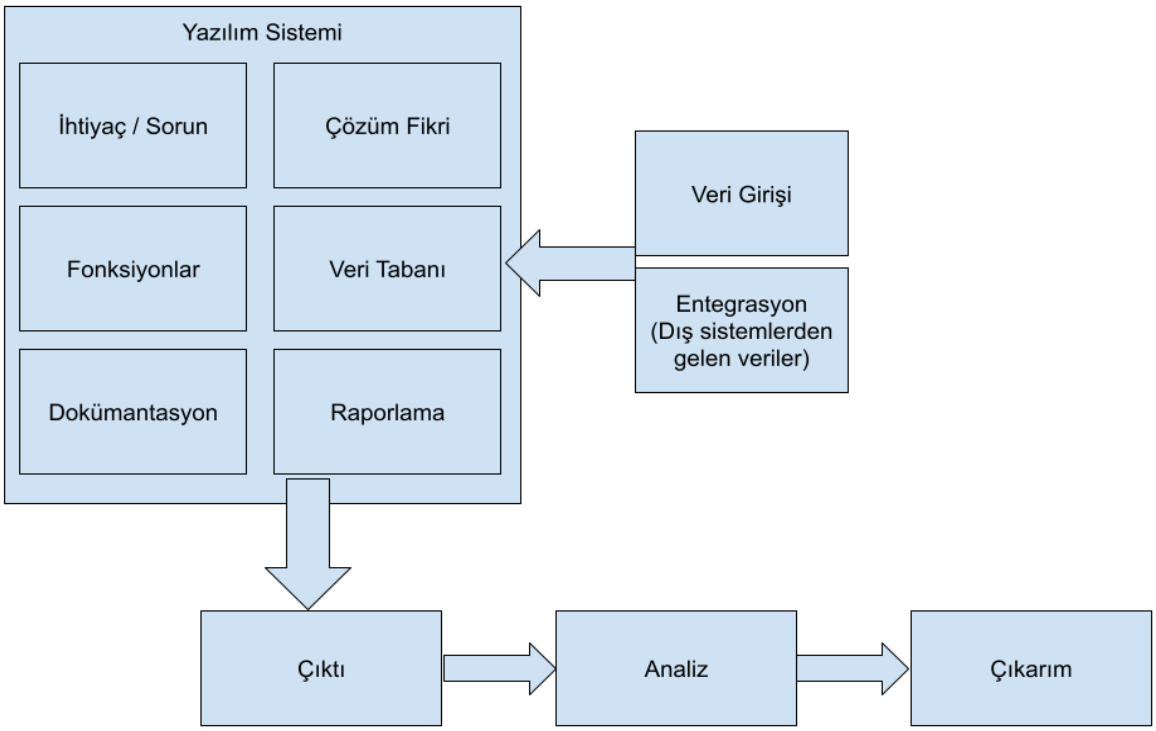
demektir. Burada verinizi sizden daha iyi koruyacağını iddia eden, teknik altyapısı ve hizmet yetkinliği olan profesyonel dijital uzmanlar söz konusudur. Teknik olarak hukuki çerçeve üzerine konumlanmış bu anlaşma biçimleri kişinin kendinden daha güvenli bir biçimde verilerinin korunduğunu ispatlamaktadır. Olağan durumlarda söz konusu verilerin sağlıklı bir biçimde korunacağından hiç şüphe yoktur. Fakat olağan dışı durumlarda söz konusu verilerin ulusal güvenlik çerçevesinde incelenip incelenmeyeceğinin garantisini de teknik olarak kimse verememektedir. Olası bir savaş ya da olağanüstü başka bir durumunda ülkedeki şirketlerin ve kurumların verilerinin bulutta barındığı, yurt dışına çıkmadığı ve kapalı bir sistem mantığında sadece iç güvenlik uzmanları tarafından ulaşılabildiğine emin olunması durumunda bir sorun olmayacaktır.

Özellikle yapay zekâ algoritmalarının ve yapay sinir ağlarının bu kadar geliştiği bir dönemde, askeri amaçlar için geliştirilen yapay zekâ uygulamaları ile devlet ihaleleri, kamu ihaleleri ve devlet ile iş yapan özel şirketlerin verilerinin incelenmesi durumunda, durum tespit analizinin yapılabilmesi bazı durum ve faaliyetleri önceden ön görebilecek ön görü sistemlerinin yapılmadığı düşünülemez. Bir veriden yapılacak çıkarım doğrultusunda söz konusu çıkarımı destekleyebilecek ve doğrulayabilecek diğer verilere de sahip olduğunuzda sonuca ulaşmanız ve doğru analiz yapmanız kaçınılmaz olacaktır. Buradaki amaç sistemlerimizi kapatalım ve Kuzey Kore gibi dışarıya karşı kendimizi tamamen izole edelim değil elbette, fakat kritik verilerin ne olduğunu tespit etmek ve söz konusu kritik verileri oluşturan uygulamaların yerli-milli olmasını sağlamak, kaynak kodlara, fikirlere ve datalara sahip çıkılması ekonomik espiyonaj ve siber espiyonaj açısından çok önemlidir.

Ele geçirilen verinin az olması verinin değerini tam manada göstermediği için saldırı sonucunda ele geçirilen veriler nedeniyle kamu ve ulusal düzeyde ülkemizin zarar görmesi ne kadar muhtemel ise, yasal ve ticari yollardan ele geçirilen verilerin de ülkemize zarar vermesi o kadar muhtemeldir

Üretilen yazılım mal veya hizmetlerinin kaynak kodlarının sahipliği, fonksiyonelliği ve sonuçlarının da sahipliğidir. Yazılım sistemleri sayesinde üretilen çıktının sahibi o yazılımın sahibi olup olmadığı da hukuksal olarak sorgulanmalı, çıktının kamusal bir sonuç olup olmadığı da ayrıca sorgulanırsa değerli çıkarımlar yapılabilir. Buradaki konuyu somutlaştırmak gerekirse üzerine ev yaptığımız arsanın tapusunun bizde olması, o arsa üzerindeki kamusal hakkı bize devretmeyeceği gibi, üretilen bir yazılımın ürettiği verinin çıktısı, o veriden yapılacak çıkarımların da sahipliği kamusal değerlendirilir. Bu sebeptendir ki, kişisel verileri koruma kanunu gibi kanunlar teknik disiplinler ile sosyal disiplinleri birleştiren bir çalışma ortaya koymaktadır. Verinin sahibinden veriyi işlemek için izin alan sistemler, veri işlendikten sonra yapılacak olan çıkarımların ortaya çıkardığı değerleri sahiplenmektedir ve bu konu da irdelenmesi, sorgulanması gereken bir konudur.

Şekil 3: Yazılım Sistemi (Kaynak: Yazar tarafından oluşturulmuştur)



Şekil 3'te olduğu gibi her yazılım sistemi bir ihtiyaç veya bir soruna odaklanır ve bir çözüm yöntemi veya fikri ile geliştirilir. Geliştirilen ürüne fonksiyonlar eklenir, süreç iyileştirilir ve nihai yazılım ürünü ortaya çıkar. Girdi veriler işlenir (parçalama, birleştirme, matematiksel işlemler, ayıklama), işlenen veri belli bir mantık çerçevesinde depolanır ve raporlanır. Raporlar her ne kadar sonuç olsa da ilgili raporları hazırlamak veya yorumlamak yazılım sisteminin de dışında farklı bir uzmanlık ile irdelenir. Özellikle yazılım sistemlerindeki çıktılar yetkilendirmeye bağlı olarak gösterilir ve gizlenir. Gizlilikteki temel amaç söz konusu verilerin ifşasının iç işleyişin 3. Kişiler tarafından bilinmemesinin istenmesidir. Gizlilik kavramı o kadar önemlidir ki, verileri korumak için çeşitli yazılım ve donanım yatırımları yapılır.

2.4. İş Yazılımlarının Geleceği

İş yazılımları denilince akıllara genellikle muhasebe sistemleri gelmektedir. Endüstri 4.0 ve Toplum 5.0 kavramlarının da ortaya çıkışından sonra, dijitalleşme ve dijital dönüşüm kavramları özellikle kurumsal firmaların sürekli olarak üstünde durduğu ve büyük yatırımlar yaptığı kavram olan Kurumsal Kaynak Planlaması (Enterprise Resource Planning - ERP) Sistemi kavramı ön plana çıkmıştır. Önceden temel üretim planlamaları yapmaya yarayan ERP sistemleri artık daha bütünleşik, esnek, bulutta çalışan, uyarlama ve geliştirme faaliyetleri hızlı, hantal ve bağımlılığı olmayan, mobil veya web browserlarda çalışabilecek nitelikte bir sistem arayışına girilmektedir. Özellikle Almanya ve ABD ülkelerinin domine ettiği sektörde yerli alternatiflerin de çok güçlendiğini gözlemlenmektedir. Bunun bir sebebinin de ülkemizdeki iş süreçlerinin yurt dışına göre çok daha fazla dinamik ve esnek yapısından kaynaklı, yerli üretilen yazılım çözümlerinin söz konusu esnekliğe ayak

uydurabilecek nitelikte kodlanmasıdır. Çünkü Almanya, ABD gibi ülkelerdeki iş süreçleri ve muhasebe mevzuatları, Türkiye'de olduğu gibi sürekli değişmemekte ve mevcut süreçler uzun yıllar hiç revize görmeden devam etmektedir. Dolayısıyla altyapı ne kadar esnek olursa olsun, teknolojinin sürekli geliştiği zamanlarda yeni olan her ürün eskinin yeteneklerini kapsadığı için tercih sebebi olmaktadır.

Önümüzdeki yıllarda iş yazılımlarının geleceği; yapay zeka, makine öğrenmesi, büyük veri, blok zincir, gibi kavramları da kapsamak zorunda olacağından yeni altyapılar ile geliştirilen güncel iş yazılımları çağa ayak uydurabilecek, bu teknolojileri kendi sistemleriyle doğru entegre edemeyen yazılımlar artık kullanılmayacaktır. Dolayısıyla yerli üretilen iş yazılımlarının değerlenmesi, yurt dışındaki hangi amaca hizmet ettiği belli olmayan şirketler tarafından satın alınması, yazılım sistemleri içindeki veri ve belgelerin yurt dışına yetkisiz bir biçimde çıkışının önünü açabilecektir.

2.5. Sektörün büyüklüğü ve Fon Yönetimi

Bugün dünyanın en büyük 10 şirketinin 7 si teknoloji şirketidir (Apple, Microsoft, Alphabet, Amazon, Facebook, Alibaba ve Tencent) (Keyofchange, 2022b). Bu şirketler incelendiğinde beşi neredeyse tamamen yazılım teknolokisi üretmektedir. Ülkemizde de son yıllarda artarak desteği devam eden teknokentler, teknoparklar, AR-GE merkezleri ve inovasyon teşvikleri sayesinde birçok yazılım şirketi katma değer üretmektedir. Özellikle ulusal düzeyde iş yapan ve yurt dışına yazılım ihracatı yapılması konusunda henüz tam olarak yeterli olmadığının vurgusunu sürekli olarak yapılmaktadır.

Daha önce para ve borç yaratabilmek yetkisi sadece bankalara aitti, artık bir banka olmadan özel bir kuruluşun verdiği teminat ile ödemeler alınabilmekte, para söz konusu şirket veya şirketler üzerinden alıcıdan satıcıya aktarılabilmektedir çeşitli komisyon oranları çerçevesinde aktarılabilmektedir. Özellikle söz konusu ekosistemdeki komisyon oranları, işlem hacimleri ve sürdürülebilirliğe bakıldığında çok karlı bir iş gibi gözüken bu uygulamalara daha makro düzeyde bakmak gerekirse, sistem üzerinde dolaşan para kadar değerli bir olgunun da var olduğunu unutmamak gerekmektedir (Keyofchange, 2022b).

Söz konusu para kadar değerli başka bir olgu ise, o paraya ait bilgidir. Bir paranın tutarı kadar önemli olan kısmı da nereden geldiği ve nereye gideceğinin bilinmesidir. BDDK tarafından kontrol edilebilen bankalara alternatif olarak para işlemlerini yapabilecek yetkinlikteki şirketlerin olması, hız, konfor, rekabet avantajı ve tüketicinin karlılığı düşünüldüğünde çok verimli olsa da kontrol ve denetleme yapmanın zor olduğu bu kadar esnek olan bu sistemin ileride bir güvenlik sorunu olup olmayacağının da irdelenmesi, gerekli önlemlerin alınması ve ortaya çıkabilecek sorunlarla ilgili çözüm yollarının belirlenmesi gerekmektedir.

Dünyada diğer lider yazılım uygulamalarını incelediğinizde, söz konusu yazılımların finansmanında mutlaka devlet destekleri görmekteyiz, Fakat bu destekler söz konusu hibe destekler gibi değildir, stratejik üstünlük sağlayabilmek önceden siyasi ve stratejik olarak adımları önceden bilerek yatırım ve faaliyetleri yürütebilecek güce sahip olacak kadar büyük desteklerdir. Devletin siyasi otorite olarak bir projeye destek vermesi, ülke içindeki uzman ve ekonomik güç sahibi olan herkesin ilgili projeye yatırım yapmasıyla eşdeğerdir. Sadece maddi destek dışında siyasi desteğin başka bir kazanımı da fikirden yana doğabilecek rakiplerin azalmasını sağlayacak, hatta söz konusu rakipler bile ilgili projenin paydaşları olmak için çaba sarf edeceklerdir. Uluslararası alanda muadili olan bir teknolojiyi yerli ve milli bir

şekilde üretmek söz konusu teknolojideki dışa bağımlılığı ciddi oranda azaltacağından, uluslararası rakiplerin de kaynaklarını azaltacaktır. Ülke içindeki yatırımlarını çektiklerinde doğacak iş gücü de boşta kalmayacak söz konusu projeye çok ciddi bir kazanılmış bilgi katılmış olacaktır.

En basit manada inceleyecek olursak; başarılı bir fikir ile kurulan startuplardan bazıları kitlesel fonlama kuruluşları ve melek yatırımcıların gruplarının olduğu konsorsiyumlar tarafından çok ciddi yatırımlar almakta ve bir anda devasa şirketlere dönüştürülmektedirler. 10 yıllık hedefe neredeyse 1 yılda erişebilen şirketlere yapılan yatırımların kaynaklarının araştırılması, yapılan yatırımların ve yapılan yatırımlara istinaden harcanan paraların gerçekliğini de irdelemek gerekmektedir. Özellikle kara para aklama yöntemlerinin günümüzde daha teknolojik veya yeni yöntemler ile yapıldığını akıldan çıkarmamak gerekmektedir. Genellikle nakit akışının çok hızlı olduğu sektörleri seçen kara para aklayıcıların söz konusu yazılım şirketleri paravan şirkete dönüştürebileceğini de unutmamak gerekir. Finansal şirketler ile finansal veri barındıran uygulamaların stratejik ortaklıklarına dikkat etmek, söz konusu ortaklık amacını ve yöntemini iyi irdelemek gerekmektedir. Finansal kredi puanı hesaplayan ve yasal kredi finansörleri ile kobileri birleştiren şirketlerin işleyişine mercek tutmak, hangi yöntem ve bilgilerle finansal verilerin analizinin yapıldığını araştırmak, yasal olup olmadığının çerçevesini de iyi çizmek gerekmektedir (Keyofchange, 2021).

Ülkemizdeki Sermaye Piyasası Kurulu tarafından yönetilen borsadaki yerli yazılım firmaları genellikle büyüme hedeflerine istedikleri zamanda ulaşamazlar, bunun yerine kolay yol olan şirket satışı veya büyük orandaki hisse satışı yöntemini kullanırlar. Buradaki ülke dışından gelen yatırımcılar söz konusu şirketlerin potansiyelini fark ederek ilgili şirketlere çok büyük yatırımlar yaparlar. Sonuç olarak yazılım şirketlerinin genellikle halka arz olmadığını ve direkt olarak satıldığını görmekteyiz (Webrazzi, 2014). Yerli teknoloji şirketlerini borsa da yatırımcı ararken bulmamızın zor olmasının sebebi standart değerleme araçlarıyla yazılım şirketleri değerlendiğinde doğru bir matematiksel kıymet ortaya çıkmadığını gözlemlemekteyim bu sebepten borsadaki standart yatırımcıların dikkatini fazla

çekmemektedir. Yazılım şirketleri normal eski yöntemlere göre büyümezler, geliştirdikleri kod ve kazanılmış bilgi yeri geldiğinde birçok bina veya menkul kıymetten çok daha fazla değer bulabilir. Buradan da anlaşılacağı üzere, söz konusu yazılım şirketlerinin hisselerinin alınması normal bir bakış açısına göre çok karlı değil, fakat potansiyeline doğru bakıldığında şirketin değeri, kısa süre içinde imara açılacak ucuz bir tarladan farksız olacaktır. Şirketin ürettiği yazılım sayesinde elde edilen bilgi ve belgeleri analiz ettiğinizde çok kıymetli yorumlar ortaya çıkabileceği gibi, tehlikeli yorumlar da ortaya çıkabileceği düşünülebilir.

Neticede çok değerli bir fikri çok büyük değer yaratacak bir araç haline dönüştürmek varken, çok değerli kavramları değersizleştirecek bir araç haline dönüştürmek o aracı kullananın yeteneğindedir. Bir silah korunmak için de kullanılabilir, fakat saldırmak içinde. Dolayısıyla Endüstri 4.0 sürecinde teknolojinin bu kadar gelişmesi sayesinde, ortaya bir sürü robot ve yazılım çıkmasıyla mevcut iş gücü ve emeğin azalması hedeflenmiş ve başarılı olunmuştur. Fakat ortaya çıkan kazanımların yanı sıra yan kazanım olan Toplum 5.0 Kavramının da temelinin atılmasına sebep olan değerli veri kavramı doğmuştur. Bu verinin neden bu kadar değerli olduğunu anlamak için uluslararası arenada tüm bu verileri işleyip doğru analizler çıkartmak adına Yapay Zeka ve Quantum bilgisayarlara çok ciddi yatırımlar yapıldığını izlemek gerekmektedir.

SONUÇ

Yazılım firmalarının ve dolaylı olarak bu firmaların sahip oldukları dataların satışı ile ilgili yurtiçi tekelleşmenin de önüne geçmek gerekmektedir. Son yıllarda benzer sektörlerdeki benzer firmaları toplayan finansal kuruluşların aslında uluslararası bir oluşumun dijital veya finansal tetikçisi olup olmadığı hususunda istihbarat çalışmaları yapılmalı ve faaliyetlerinin de ayrıca incelenmesi gerekmektedir. Uluslararası düzeyde istihbarat şirketlerinin bu gibi oluşumları dijital veya finansal tetikçi olarak kullanmasının önünde yasal bir önlem alınmaması durumunda, kaynağı nereden geldiği belli olmayan paraların şirket alımlarındaki aklama faaliyetlerine göz yumulmuş olacağı aşikârdır. Faaliyetler gerçekleştikten sonra tespit etmek, yurt içindeki stratejik planların, yurt dışında bulunan istihbarat şirketlerine bir yaptırımın uygulanamaması demektir. Söz konusu hasarı tespit etmek için ise ne kadarlık bir verinin ifşa edildiğini tespit etmek demek olduğu için, sadece bunun için bile çok uzun soluklu teknik çalışmalar yapmak gerekecektir. Son yıllardaki teknolojik gelişmeler ışığında, teknoloji üreten şirketlerin hızlı bir ivme ile gelir elde etmesi yabancı sermayenin dikkatini çekmeyi başarmıştır. Ticari amaç için yapılan bu satın almaların, daha fazla oranda kâr elde etmek ve gelir düzeylerini artırabilecek potansiyeldeki şirketlere sahip ana kazanımlardan biri gibi gözükse de aslında sahip olunan verinin kıymetinden dolayı kazanılan para miktarı yan kazanıma dönüşmektedir.

Geçtiğimiz yıllarda yabancı sermayenin, ülkemizdeki enerji ve doğal kaynaklar ile üretim yapan şirketleri satın alma eğilimleri oldukça fazla olduğu görülmüştür. Şirketlerin kuruluş ve işleyişlerinde start-up ruhunun kaybolmasından sonra belirli bir standartlaşma ve hantallaşma olduğu işletme yönetimi kapsamında incelendiğinde oldukça olağan bir durumdur. Özellikle gelir ve gider mekanizmasını belli bir standarda oturtmuş her kurum, piyasada ne kadar agresif davranırsa davransın, kendi iç dinamiklerini sürekli iyileştirme metotlarını uygulasa bile artık verimli bir hale dönüştüremez duruma gelebilir. Özellikle kurumsallaşmanın kıyısında dolanan şirketlerin sert ekonomik koşullarda, enflasyonun sürekli olarak arttığı, gerçek değerlemelere dayanmayan enflasyon artışları karşısında yaptığı zamlar ve satışlar,

karlılığı azalmaktan kurtaramayacaktır. Ülkemizdeki enflasyondan kaynaklı birçok kurum veya kuruluşun karlılığı azalmaktadır. Bunun farkında olan yabancı sermayenin, ülkedeki para biriminin değersizliğinden kaynaklı kendi para birimiyle satın alma gücünün yüksek olduğu bir piyasada karlılık riskinin minimum olması da ayrıca kaçınılmazdır. Söz konusu yabancı sermayeli şirketlerin ülkemizdeki söz konusu yazılım şirketlerini satın almaları ve tüm süreçlerini daha da otomatize etmelerinin sadece kârlılık olmadığı görülmektedir.

Yazılım sektöründeki tekelleşme, siber güvenlikle ilgili çeşitli sorunlara yol açabilir. Birincisi, büyük teknoloji şirketlerinin pazarın büyük bir kısmını kontrol etmeleri, siber saldırılar karşısında savunmasızlığı artırabilir. Rekabetin sınırlanması, inovasyonu azaltabilir ve güvenlik açıklarının daha yavaş bir şekilde kapatılmasına neden olabilir. Aynı zamanda, tek bir devasa şirketin siber güvenlik standartlarını belirlemesi, sektör genelinde çeşitliliği ve esnekliği kısıtlayabilir. İkincisi, bu tekel haline gelen şirketlere finansal bir avantaj yaratabilir. Finansal avantajın ulusal güvenlik kapsamında değerlendirmek için uluslararası finansal ve ekonomik tetikçiliğin geldiği noktayı da bilmek gerekir. Toplumun refah seviyesini tehdit edecek her türlü önlemi almak için finansal kredi puanlarını tespit edebilecek düzeyde bir veriye sahip olmak, stratejik açıdan karşı ülkeye karşı avantaj sağlamak demektir. Askeri düzeydeki stok seviyesini ve finansal bilgileri ifşa etmesek bile, ülke içi piyasalardaki hareketlerin ifşa edilmesi durumunda mevcut durum analizini yapmak karşı ülke istihbaratı açısından oldukça verimli sonuçlar elde edecektir. Yazılım şirketlerinin verilerinin ve bu şirketlerin kendilerinin uluslararası kuruluşlar tarafından domine ediliyor olması istihbarata karşı koyma kapsamı açısından dezavantajlı bir durum yaratmaktadır.

Sonuç olarak, ulusal boyutta bir bilgi veya data sızıntısının önüne geçebilmek için, üretilen her yazılımın veya uygulamanın amaç ve kapsamını doğru değerlendirebilecek nitelikte analizler yapılmalı. Satış veya satın alma faaliyetlerinden önce sebep ve sonuçlar iyi irdelenmeli, Sektördeki alanındaki uzmanlardan veya devlet kademesindeki uzmanlardan görüşler alınıp, gerekiyorsa satış ve satın alma faaliyetlerinin irdelenebilir.

Sermaye piyasaları kurulu özellikle yazılım şirketlerinin halka açılması ile ilgili süreçleri kolaylaştırması, şirketlerin yatırımcıyı dışarıdan bulmasının önünü kapatacaktır. Özellikle halka açılan ve yatırım bulabilen şirketler hisse satışı konusunda temkinli olacak ve doğal büyüme mekanizmasını devreye sokacaktır. Ulusal düzeyde söz konusu durum ile başa çıkmak için alınan önlem örneklerinden söz etmek gerekirse, yazılım sektörüne ait gelir ve gider mekanizmalarında vergi avantajları metotları oluşturmak faydalı olacaktır. Sermaye Piyasası kurulunun şirket değerleme yöntemlerini daha yeni nesil yöntemlere göre yenilenmesi, dolayısıyla potansiyeli yüksek yazılım şirketleri sermaye ve yatırım için şirketi satmak zorunda kalmadan gerçek değerlemeyle halka arz süreçlerine yönlendirme yapılmasının sağlanması söz konusu şirketlerin finans bulmak için yurt dışına açılmasının önüne geçebilir, veri barındıran, taşıyan ve işleyen yazılım şirketlerinin. Söz konusu faaliyetleri nedeniyle sürekli olarak incelenmesi, barındırdığı verinin içeriğinden ve güvenliğinden sorumlu olduğunun bildirilmesi, şirket satış veya devirlerinde işlenen verinin söz konusu satışa dâhil olmamasının hem yasal hem de teknik olarak sağlanması siber espiyonajın çok büyük oranda önüne geçecektir.

Ulusal düzeyde bir siber güvenlik politikasının belirlenmesi ve sertifikalandırma süreçleriyle ilgili prosedürlerin oluşturulması sürecin yasallaşmasının önüne geçer. Bu sayede siber güvenlik politikaları devlet siber kurumları tarafından daha kolay uygulanabilir. Sadece suç

teşkil eden faaliyetlerin değil, tehlike oluşturabilecek nitelikteki verilerin korunmasının sağlanmasına yönelik önlemlerin alınması gerekir hayati önem taşıdığından yerli büyük teknoloji şirketlerinin bulut bilişim altyapısı oluşturulmasına yönelik teşvik ve yaptırımların uygulanması gerecektir. Bu doğrultuda devlet destekleri mekanizmalarını artırarak dijitalleşmenin yerlileşmesi büyütülür.

Bugün kamu kurum ve kuruluşların finansal hareketleri sayıştay tarafından denetlendiği gibi, özel kurum ve kuruluşların da finansal hareketleri gelir idaresi başkanlığı tarafından denetlense bile, söz konusu denetlemeler sadece vergilendirme veya suç teşkil edebilecek potansiyel finansal hareketler çerçevesindedir. Ya da kamu ihale kanununun gereklerinin yerine getirilip getirilmediği ile ilgili çalışmalar ve suç tespitleri yapılmaktadır. Fakat finansal hareketlerden sadece ulusal anlamda güvenliği tehdit edebilecek nitelikte çıkarımlar da yapılabilir. Yurtdışından sürekli olarak ithal edilen bir mal veya hizmetin ya da sürekli olarak yurt dışına satışı yapılan bir mal veya hizmetin geriye dönük irdelenmesi yerine, hareketin olduğu anda veya çok kısa bir zaman sonrasında o veri hareketi ile ilgili çıkarımlarda bulunulacak yapay zekâ uygulamalarını yerli ve milli bir şekilde geliştirmek gerekmektedir. Veriyi anlayabilecek ve yorumlayabilecek uzman ekipler tarafından verinin ham halinin incelenmesi ve çıkarımlar yapılması teorikte ve pratikte uzun sürebilir. Fakat bu amaç doğrultusunda geliştirilmiş bir yapay zekâ uygulaması dijital tetikçiliğe karşı ve dijital istihbarata karşı bir istihbarat silahı olarak kullanılabilecektir. Ortaya çıkan sonuç tablosuna göre, geçmiş alışkanlıklarımızı bir kenara bırakmak, olay olduktan sonra ortaya çıkan zararın sebeplerini tespit etmeye çalışmaktan ziyade problemlerin olmadan önce tespit edilebilmesi ve halkın bu yönde bilinçlenmesi için halkla ilişkiler çalışmaları yapılması gerekmektedir.

Kaynaklar

Acar, Ü. (2011). İstihbarat. Akçağ Yayınları.

Atan, S. (2016). Veri, büyük veri ve işletmecilik. Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 19(35), 137-154.

Deloitte, (2021). Türkiye'de yazılım ekosisteminin geleceği. Erişim tarihi: 12 Kasım 2023. https://www2.deloitte.com/tr/tr/pages/consulting/articles/turkiyede-yazilim-ekosisteminin-gelecegi.html

Demircioğlu, İ., Güven, O., ve Hınız, Y. (2021). İslâmiyet'in kabulünden sonra türklerde istihbarat felsefesi. Güvenlik Bilimleri Dergisi (2. Uluslararası Güvenlik Kongresi Özel sayısı (İstihbarat ve Güvenlik)): 15-34.

Doğan, K. ve Arslantekin, S. (2016). Büyük veri: önemi, yapısı ve günümüzdeki durum. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 56(1): 15-36.

Dulles, A. W. (2007). The Craft of Intelligence. USA, Manas Publications.

Economic Espionage Act Of 1996 (https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf)

Fastcompany (2023, Mart). Türkiye'nin en büyük 100 internet şirketi. Erişim tarihi: 02 Aralık 2023. https://fastcompany.com.tr/dergi/turkiyenin-en-buyuk-100-internet-sirketi-2023/

İslah, E. (2023). Yazılım endüstrisinde faaliyet gösteren firmaların değerini etkileyen faktörlerin tespit edilmesi: Nasdaq'da işlem gören yazılım üreticisi firmalar üzerinde uygulamalı bir yaklaşım. Doktora Tezi. Osmaniye Korkut Ata Üniversitesi, Osmaniye.

Keyofchange (2019, Aralık). Türkiye'deki FinTech yatırımları 12M $. Erişim tarihi: 02 Aralık 2023. https://www.keyofchange.com/tr/2272/T%C3%BCrkiye%E2%80%99deki%20FinTech%20yat%C4%B1r%C4%B1mlar%C4%B1%2012M%20%24/)

Keyofchange (2021, Ekim). Startup'lar için belirlenen 10 yıllık hedefe 15 ayda ulaşıldı. Erişim tarihi: 02 Aralık 2023. https://www.keyofchange.com/tr/2391/Startup%E2%80%99lar%20i%C3%A7in%20belirlenen%2010%20y%C4%B1ll%C4%B1k%20hedefe%2015%20ayda%20ula%C5%9F%C4%B1ld%C4%B1/

Keyofchange (2022a, Nisan). "Pulse of Fintech" Raporu. Erişim tarihi: 02 Aralık 2023. https://www.keyofchange.com/tr/2412/%E2%80%9CPulse%20of%20Fintech%E2%80%9D%20Raporu/

Keyofchange (2022b, Nisan). Yazılımda hizmet ihracatı. Erişim tarihi: 02 Aralık 2023. https://www.keyofchange.com/tr/2420/Yaz%C4%B1l%C4%B1mda%20Hizmet%20%C4%B0hracat%C4%B1/

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. Sustainability, 13(24): 13677.

Köken, E. ve Gül, İ. (2020) Casusluk Faaliyetleri ve Uluslararası Casusluk Suçu(https://acikerisim.kku.edu.tr/xmlui/bitstream/handle/20.500.12587/13650/1d47dd0e-c0f1-4b2a-a532-8dabda879073.pdf)

Köse, Ş. (2019). İstanbul'da yazılım sektörünün yerseçim tercihleri. Yayımlanmamış Yüksek Lisans Tezi. İstanbul Teknik Üniversitesi, İstanbul.

Map (2022, Temmuz). Bulut bilişim istatistikleri. Erişim tarihi: 02 Aralık 2023. https://www.map.com.tr/tr/bulut-bilisim-istatistikleri-2022/

Moro-Visconti, R. (2022). The valuation of trademarks and digital branding. In The Valuation of Digital Intangibles: Technology, Marketing, and the Metaverse 285-319.

PwC (2022). Fintech Nedir? Erişim tarihi: 02 Aralık 2023. https://www.pwc.com.tr/fintech-nedir

Riley, K. J., Treverton, G. F., Wilson, J. M., & Davis, L. M. (2005). State and Local Intelligence in the War on Terrorism. RAND Corporation.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2): 53-72.

Tang, A., Aleti, A., Burge, J., & van Vliet, H. (2010). What makes software design effective?. Design Studies, 31(6): 614-640.

UNCTAD. (2012). Information Economy Report 2012: Digitalization, Trade and Development. Geneva: UNCTAD.

USOM (2014, Temmuz). Siber güvenliğe ilişkin temel bilgiler. Erişim tarihi: 13 Kasım 2023. https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf

Webrazzi (2014). Pozitron'un satışı ve neden yazılım şirketleri halka açılmıyor? Erişim tarihi: 02 Aralık 2023. https://webrazzi.com/2014/02/05/pozitron-satisi-neden-yazilim-sirketleri-halka-acilmiyor

Yücelik, R. (2015). Ekonomik istihbarat modellemesi ve yükselen ekonomiler için öneri

(https://acikbilim.yok.gov.tr/bitstream/handle/20.500.12812/95605/yokAcikBilim_10089014.pdf)

Yazar Hakkında

HAKTAN AKDAĞ

EĞİTİM:

Dokuz Eylül Üniversitesi Bilgisayar Programcılığı Önlisans Programı :2009

Anadolu Üniversitesi İşletme Lisans 2013

Anadolu Üniversitesi Yönetim Bilişim Sistemleri Lisans 2021

Dokuz Eylül Üniversitesi Toplam Kalite Yönetimi Yüksek Lisans 2023

MESLEKİ BİLGİLER:

Univera Bilgisayar Sistemleri A.Ş 2010-2015 - İş Zekası Uzmanı & Yazılım Geliştirici

Aydın Büyükşehir Belediyesi Kamu İştirakleri - AYBEL A.Ş - EGEET A.Ş 2016-2019 - Bilgi Teknolojileri Yöneticisi

Dokuz Sistem Bilişim San. Tic. Ltd Şti - 2019 - Devam Ediyor - Kurucu & Kıdemli Yazılım Geliştirici

ATIF İÇİN:

Akdağ, H. (2024). Yazılım Sektöründeki Şirketlerin Yabancı Şirketlere Satılmasının İstihbarat ve Siber Güvenliğe Etkisi. Erişim tarihi: xx.xx.xxxx., https://www.teram.org/Icerik/yazilim-sektorundeki-sirketlerin-yabanci-sirketlere-satilmasinin-istihbarat-ve-siber-guvenlige-etkisi-257

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Email : teramarastirmamerkezi@gmail.com