

DIGITAL GAME AND INTELLIGENCE RELATIONSHIP

M. Fatih Sezgin - Ömer Gök - Kazım Ongun

Abstract

Digital games have started to show their presence in every aspect of our lives. Today, individuals of all ages, from the age of 7 to the age of 70, now spend an important part of their time on these digital platforms, sometimes for entertainment, sometimes for financial gain. These delays can lead to undesirable results. It is possible to establish friendships with the people in the virtual world in front of us or next to us, without knowing their real-world identities, and share the most private information willingly or unwillingly.

The relationship between the digital world and intelligence begins to be interrelated at the point of revealing the purposes behind secret friendships. The information received during the game, both live in the game and before or after the game, through sociological methods, shared spatial information, and serious data sharing from the individual to the country. In these platforms, it appears in the form of sharing information in a deep and wide spectrum, ranging from the aims of obtaining financial gain from the organizations and or the organizational staff, from their goals to the goals of obtaining moral gain. The relationship between digital game markets, which is a new subject in our country, and intelligence, which has only been found in a study so far, has been tried to be examined. The effect of intelligence, which is the most private point of the states, on the digital world and games, the struggles of China, Russia and the USA in the digital world are explained with examples. The fact that the companies in the digital game market are supported by the state and how much effect they have on the market economically have been revealed by the data.

Keywords: *Game, mobile game, digital game, intelligence, cyber intelligence.*

DİJİTAL OYUN VE İSTİHBARAT İLİŞKİSİ

M. Fatih Sezgin* - Ömer Gök - Kazım Ongun*****

Öz

Dijital oyunlar hayatımızın her alanında varlığını göstermeye başlamıştır. Günümüzde 7 yaşından 70 yaşına kadar her yaştan bireylerin bu dijital platformlarda, kimi zaman vakit geçirme, kimi zaman eğlence, kimi zamanda maddi çıkar amaçlı olarak zamanlarının önemli bir kısmını harcamaktadırlar. Bu vakit geçirmeler istenmeyen sonuçlara sebebiyet verebilmektedir. Karşımızdaki ya da yanı başımızdaki sanal dünya ki kişilerin, gerçek dünyadaki kimliklerini bilemeden onlar ile dostluk kurulabilmekte, en mahrem bilgileri isteyerek ya da istemeyerek paylaşabilmektedir.

Dijital dünya ile istihbarat arasındaki ilişkide, gizli dostlukların arkasında yatan amaçların ortaya çıkarılmasını noktasında birbiri ile ilişkilenebilir. Gerek oyun içerisinde canlı olarak gerekse oyundan önce veya sonra bağlantı yöntemleri vasıtasıyla, sosyolojik yöntemler ile oyun sırasında alınan bilgiler, paylaşılan mekânsal bilgiler, bireyden ülkeye uzanan ciddi veri paylaşımlarıdır. Bu platformlarda örgütlerin ve veya örgüt elamanından maddi kazanç elde etme, amaçlarından manevi kazanç elde etme amaçlarına kadar uzanan derin ve geniş bir yelpazede bir bilgi paylaşımı şeklinde önümüze çıkmaktadır. Ülkemizde yeni bir konu olan dijital oyun piyasaları şimdiye kadar tek çalışmaya rastlanmış olan istihbarat ilişkisi irdelenmeye çalışılmıştır. Devletlerin en mahrem noktası olan istihbaratın dijital dünyada ve oyunlara etkisi, bu konuda Çin, Rusya, ABD'nin dijital dünyadaki mücadeleleri örnekler ile anlatılmış, J.Snowden'in ifşalarından dijital dünyanın da bu konuda kullanıldığı gerçeği ile, devletlerin bu konudaki çalışmaları örnekler yorumlanmaya çalışılmıştır. Dijital oyun piyasasındaki firmaların devlet destekli olmaları ve ekonomik olarak piyasada ne kadar etkiye sahip oldukları veriler ile ortaya koyulmuştur. Ülkemizde bu konuda gerekli insan kaynağına yatırımın önemi ve güvenlik açısından farkındalık yaratılmasının gerekliliği vurgulanmaktadır.

Anahtar Kelimeler: *Oyun, mobil oyun, dijital oyun, istihbarat, siber istihbarat.*

* Doktorant-Uluslararası Güvenlik, mfsezgin@gmail.com <https://orcid.org/0000-0001-8030-2479>.

** Doktorant-Hukukçu, krmbay@gmail.com <https://orcid.org/0000-0003-1135-7470>.

*** Jandarma Personeli, Artvin İl Jandarma Komutanlığı, ongun.kazim@gmail.com <https://orcid.org/0000-0002-9993-5572>.

Bu makaleye atıf için: Sezgin, M. Fatih, Gök, Ömer ve Ongun, Kazım. (2023). Dijital Oyun ve İstihbarat İlişkisi, SDE Akademi Dergisi, 3(2), 181-216

GİRİŞ

İnsan oğlunun dünyaya geldiği ilk günden beri, topluluklar arasında mücadele ve bu mücadeleler için kullandıkları araçlar vardır. Zamansal ve Teknolojiye bağlı olarak bu araçlar her ne kadar değişse de amaç hiçbir zaman değişmemekte, üst olma, daha zengin olma, daha çok bilgiye erişme, daha güçlü olma gibi hedefler ve arzular ile hareket edilmektedir. İnsan oğlunun bu amacını gerçekleştirmek için zamanla geliştirdiği ve adına istihbarat denilen olgu ile hareket etmeye başlamış ve hedeflerine ulaşmak için istihbarat aracını da kullanmıştır.

Tanım olarak İstihbarat; “Devlet tarafından belirlenen ihtiyaçlara karşılık olarak çeşitli kaynaklardan derlenen haber, bilgi ve dokümanların işlenmesi sonucu elde edilen üründür” (MİT, 2021). Bir diğer tanımda istihbarat: “Hükümetlerin, askeri grupların, işve diğer grupların sistematik olarak rakiplerinin yeteneklerini ve niyetlerini keşfetmek amacıyla bilgiler toplayıp değerlendirdikleri süreçtir (Fidan, 1999: 20). İstihbarat ile ilgili ilk olarak tarihi süre. İncelendiğinde, ilk olarak resmi bilgilere M.Ö. 2000 yıllarında Fırat nehri kıyılarında rastlanmaktadır. Bannum isimli komutanın, bir kil tablette yabancı sınırlarında ateşler yakıldığını ve bunun ne manaya geldiğini bulmalarını istediği görülmektedir. M.Ö. 500 yılında Perslerden sartlaplık sistemini aslında iç istihbarat toplamak için kullandıkları bilinmektedir. M.Ö. 300 yıllarında Kautilya'nın kraliyet yönetimi için bir rehber olan Arthashastra'da kale inşaatlar, fil yetiştiriciliğinin yanında, tüccar casuslardan, gezgin ajanlardan, din adamı ve dilenci rolündeki ajanlardan bahsetmektedir. Büyük İskender komutanları hakkında, sürekli istihbarat toplatmıştır. Antik Yunanlılar, şifreli mesajlaşmanın ilkel yöntemlerini uygulamıştır M.Ö. 55 yılında Sezar'ın İngiltere'yi işgalinde istihbarat kullanmıştır (Liulevicius, 2011: 13). Sun Tzu'nun; “Bilge hükümdarla, iyi bir komutanın normal askerlere oranla kolaylıkla savaş kazanıp, zafere ulaşması istihbarata bağlıdır (Tzu, 2008: 73). İstihbarat ve casusluk faaliyetleri siyasi iktidarlar ve devletlerin varlıklarını sürdürebilmeleri için tarih boyunca her zaman var olmuştur. Machiavelli, The Prince ve The Art of War adlı eserinde; yöneticilerin ellerindeki gücü, çıkarı

korumak için her daim casusluk ve istihbaratı kullandığını savunmaktadır (Machiavelli, 1994: 100-160). Flavius vegetius renatus, Roma savaş sanatı eserinde, istihbaratın savaş alanlarındaki kullanımını yönelik ciddi ipuçlarını vermektedir.

Temelde askeri ve yöneticiye notlar olan kitabında, komutanların seçiminde, savaş alanlarına ve düşman hatalarına kadar alanda istihbaratın kullanımına ve önemine yer vermektedir. (Renatus, 2019: 107-140). 1500 yıllarda Avrupa tarihinde casusluk ve istihbarat faaliyetlerine rastlanılmaktadır. Montesquies, “bir monark’ın casusu olmalı mıdır” sorusunu sorar ve “Prens bilseydi” üzerinden kurumsal istihbaratı yerer (Montesquieu, Kanunların Ruhı, Bölüm 2 XII.23 Monarşideki casuslar hakkında, 1748). 1600’lü yıllarda Avrupa’ da Venedik, Osmanlı ile ilişkilerinde özellikle istihbarat ve faaliyetlerine önemli yer vermiştir. İngiliz diplomat Sir Henry Wotton, dönemin elçilerini, ülkesinin iyiliği için yalan söylemek üzere yurt dışına gönderilmiş dürüst adam olarak tanımlamaktadır. Döneminde en gizli ve derin açıdan grubun Venedik ajanları oldukları ve Osmanlı topraklarında tüccar kimliği ile gezen birçok kişinin, Venedik gizli servisi personeli olduğu ortaya çıkarılmıştı. 1533 yılında Cenevizli Andre Doria’ya Osmanlı hakkında bilgi toplanması için emirler verildiği belgelere yansımaktadır (Jordanou, 2019: 111-150). Türk tarihinde istihbarat her zaman kullanılmıştır. Göktürk yazıtlarında bile istihbarat ve istihbaratçıların varlığına yer verilmiştir. Gözcü olarak “kargu”, haberci olarak “sabçı” tanımlamaları bu yazıtlarda geçmektedir. İslam dünyasında istihbarata önemin Hulefa-i Raşidin döneminde önem verildiği görülmektedir. Düşman hakkında raporlar alınması,” Kaysariyye” savaşında yakalanan casusların kullanılması bu dönem denk gelmektedir. Gazneliler ve Emevîler” Berid” teşkilatını kurmuş ve kullanmıştı. Selçuklularda “Berid” teşkilatını devam ettirmiş, Nizam-ül mülk, Berid teşkilatından ve “sahib-i haberler” tayininden bahsederken istihbaratın önemi vurgulamıştır (Delibalta, 201: 25-518). Fransız devrimi ile Osmanlı’da istihbarat Avrupai tarza geçmiş ve kurumsallaşmış bir istihbarat kültürüne evrilmiştir. Askeri ateşler ile Avrupa incelenmiş ve modern istihbarat Osmanlıya yerleşmeye başlamıştır (Şimşekler, 2022: 50-60). Birinci dünya savaşında Osmanlının istihbarat

faaliyetlerine önem verdiği, Ahmet Cemal Paşa'nın, Lübnan, Beyrut, Halep gibi vilayetlerde, Medine ve Mekke bölgesinden Fransızlar başta olmak üzere bölgeyi işletmiş ve önemli ödenekler tahsis etmiştir (Akyürek, 145: 2019). Napolyon, "Doğru ve yerinde kullanılan bir casus, savaşta iki yüz bin kişiye bedeldir" demiştir (Kavsıracı, 2020: 711). Birinci dünya savaşında gazete dergi, telgraf, telefon, takma diş, tren vagonu, hediye paket, sigara kâğıdı gibi yöntemler kullanılarak istihbarat faaliyetlerinde bulunulmuştur (Özkaya, 2006: 347). Osmanlıda telgraf ve gazeteler istihbarat unsuru olarak kullanılmıştır. Fotoğrafçıların casusluk faaliyetlerinde kullanıldığı raporlarda belirtilmiştir (Şimşekler, 2022: 215-217).

1. ALANLARINA GÖRE İSTİHBARAT

İstihbarat temelde iki kaynağa dayanmaktadır. HUMINT ve SIGINT. HUMINT; bilgi toplamak için insan kaynağıdır (İnsan zekâsının istihbarat için kullanılması dâhil). Bir diğer istihbarat toplama şekli ise SIGINT'tir. SIGINT özetle elektriğin ve iletimin beraber kullanılmaya başlandığı tarihteki ilk günden beri kullanılan ve sinyal istihbarat olarak özetlenen istihbarat türüdür (Liulevicius, 2011: 5). HUMINT, bilgi toplamak için insan araçları kullanır. Tarihte ilk insan grubunun bir diğeriyle karşılaştığı ve birbirlerini gözlemlemeye başladığı andan itibaren tarihte var olmaya başlamış olana HUMINT, temelde kurnazlık, incelik, kibarlık, hile, hızlı düşünme ve iki yüzlülük, yalan ve hileli yönlendirme, doğaçlama gibi insani kavramaları ön planda tutan bir bilgi toplama yöntemidir. SIGINT ise iletişimin kırılması, teknik araçlar ile dinlenilmesi ve çözümlenmesi, şifrelerin kırılması gibi temelde basit işlemlerden siber uzaydaki savaşlara kadar geniş yelpazede işlem yapan bir yöntemdir. Zamanla kendi içerisinde Elektronik istihbarat olan ELINT'in ortaya çıkmasını sağlayan, kimi zamanda düşmana karşı yanlış bilgi yayma (dezenformasyon), düşmanı hataya yâda planını ortaya çıkarmaya yönelik çalışma yürütülen bir bilgi yöntemi olarak tanımlanabilmektedir (Liulevicius, 2011: 6). GEOINT, MASINT, OSINT, SIGINT, TECHINT, CYBINT/DNINT, FINIT, SOCMINT Meteorolojik istihbarat, günümüzde uluslararası literatürde ve uluslararası arenada kullanılan diğer istihbarat türlerindedir (Tekin, 2016: 8).

GEOINT, görüntü, görüntü zekâsı (IMINT) ve jeo-uzamsal bilginin entegrasyonundan gelişen bir istihbarat türüdür. Görüntü: Doğal yâda insan yapımı nesne, etkinlik ve benzerliğin, uzaydaki yâda uzay yakın konumlandırılmış noktalardaki uydu, hava platformu, insansız hava aracı ve veya benzer platformlar tarafından üretilen benzerlikler ve sunumlar dâhil olmak üzere elde edilen bilgilerin olarak tanımlanır. Görüntü İstihbaratı ise; elde edilen bu bilgilerin yorumlanması ve analizidir. Jeo uzamsal bilgi; Bilgi edilen araçlardan, yeryüzü ya da herhangi bir coğrafi noktanın özelliklerini tanımlayan bilgi, haritalama, tanımlama ve teknolojik bilgi edinilmesidir. Coğrafi veriler teknolojik olarak işlendikten sonra analiz edilir, zaman hareket açısından birleştirilir ve dinamik etkin ürünler olarak analize sunulur (NGIA,2006: 8).

MASINT; Ölçüm ve imza istihbaratı 1950'lerde literatüre kazandırılmıştır. İkinci dünyası döneminde akustik dinleme, düşman topçusu yeri belirlenme gibi askeri amaçlı istihbarat faaliyetlerinden, radar tespit etme temelli olarak, Sovyetler birliği tarafından, Çin nükleer kabiliyetini anlamaya yönelik olarak MASINT alt disiplinin gelişmesi ve ortaya çıkması sağlandı. Radar, Nükleer, Akustik MASINT olarak alt dallara ayrılan MASINT derinlemesine analiz isteyen bir istihbarat türü olarak ortaya çıkmıştır (Lowenthal, 2016: 159-164).

Açık Kaynak İstihbaratı olarak tanımlanan OSINT, bilgi edinme faaliyeti olarak tanımlanabilmektedir. İhtiyaç olunan bilgi aranır, bilginin içeriği diğer bilgiler ile karşılaştırılır ve uygun olup olmadığı belirlenir. OSINT, yasal ve bariz bir kaynaktan bilgi edinilmesi olarak tanımlanabilmektedir. Açık kaynak istihbaratının ana avantajı, nicelik, kalite ve şeffaflık, çeşitlilik, kullanım kolaylığı ve düşük analiz maliyeti dâhil olmak üzere bilgi edinme hızıdır. Bu, bilgi teknolojisi devriminin ve İnternet'in gelişiminin sonucudur. Mobil cihazlar ve geniş bant bağlantıları gibi gözetim araçlarıyla, varlıkların izlenmesi ve analizi dünyanın her yerinden mümkündür. Araştırmacı gazeteciler bazen istihbarat servislerinden daha fazla bilgi rapor ederler. Bu nedenle OSINT ile bilgi izleme, özel servislerin faaliyetleri için çok önemlidir (Ziolkowska,2018: 68-70).

Ülkemizde de akademik alanda istihbarat alanları çeşitli şekilde tanımlanmakta ve açıklaması yapılmaktadır:

a.) Siyasi İstihbarat: Bir ülkenin siyasi yapısını oluşturan, devlet yönetim sistematığının anayasal düzen içerisinde faaliyet yürüten unsurlara karşı yapılan istihbarat faaliyetleridir.

b.) Askeri İstihbarat: Savunma sistemleri içerisinde yer alan deniz, hava ve kara kuvvet yapısı bunların yetenekleri ve kapasiteleri konularında yapılan istihbarat faaliyetleridir.

c.) Ekonomik İstihbarat: Ülkenin genel ekonomik kapasitesini, zayıf ve güçlü yanlarını, amaçlarına ulaşım ulaşamayacağını, silahlı kuvvetlerini sınırlı ve sınırsız destekleme derecesinin tespiti, finans yapısı, sanayi ve tarım vb. politikalarının tespitine yönelik yapılan istihbarat faaliyetleridir.

d.) Sosyal İstihbarat: Sosyolojik yapı çerçevesinde icra edilen bilgi toplama ve bunu analiz etme faaliyetidir. Sosyal İstihbarat sekiz temel alana yönelir nüfus, sosyal karakteristik, kamuoyu, eğitim, dini değerler, sağlık ve sosyal güvenlik sistemi, kültürel özellikler ve zihniyet analizidir.

e.) Coğrafi İstihbarat: Askeri operasyonel faaliyetlerin kapsam itibarı ile fiziksel ve kültürel çevre yapısının tespitine ve analizine yönelik çalışmalardır.

f.) Biyografik İstihbarat: Bir ülkede kültürel, ekonomik, siyasi, askeri seçkinler ve potansiyel öneme sahip bireylerle terör örgütü/suç liderlerine yönelik özel ve kamusal nitelik taşıyan bilgi toplama faaliyetidir.

g.) Ulaşım ve İletişim İstihbaratı: Ülkenin sivil ve askeri ekonomik nakil gücüne bağlı ulaşım altyapısı ve iletişim kanallarına yönelik yapılan istihbarat faaliyetidir.

h.) Bilimsel ve Teknik İstihbarat: Ülkenin ve milletin bilimsel, teknik kapasitesi buna bağlı olarak faaliyetlerinin tespitine yönelik yapılan istihbarat faaliyetidir. Savunma sanayi sektöründen tarım, ilaç vb. sektörler de bu faaliyetlerin bilimsel ve teknik verilerle desteklenerek yapılmasıdır.

ı.) Siber İstihbarat ve Enformasyon Savaşları: Teknolojinin gelişmesi ile standart istihbarat alanına giren ve yukarıda bahsedilen alana siber ve

enformasyon alanından bahsedilmemektedir. İnternete bağlı bilgisayar ve mobil cihazlar, veri tabanları, enformasyon merkezleri, çevrimiçi sistemlerin oluşturduğu alanlara “siber alan” denilmektedir. Siber alan iletişim merkezleri, petrol, doğalgaz, bilgi teknolojileri ve iletişim sistemleri, karayolu ve demir yolu ulaşım sistemleri bunlara dâhildir. Siber alanda güvenlik faaliyetlerini oluşturan sistemlere yapılacak istihbarat, karşı istihbarat ve savunma reflekslerin tümüne karşı yapılacak saldırılara “enformasyon” savaşı denilmektedir (Özdağ, 2018).

2. DİJİTAL DÜNYA VE DİJİTAL İSTİHBARAT KAVRAMLARI

İnternet, bilgisayar ve iletişim dünyasında daha önce hiç olmadığı kadar devrim yarattı. Telgrafın, telefonun, radyonun ve bilgisayarın icadı, bu benzeri görülmemiş yetenek entegrasyonu için zemin hazırlamıştır (Liener vd. 1997: 83). İlk internet bağlantısı Amerikan ordusunun kendi içerisinde güvenli bir iletişim ağı oluşturmak amacıyla 1960’lı yıllarda yapılan bir projeye dayanmaktadır. Bu projeye dünya geliştikçe ve zaman geçtikçe yeni ağlar ve yeni bilgisayarlar eklenmiş askeri projeler dışındaki kullanıcılarda eklenmeye başlanmış ve yararlanmaları sağlanmıştır. Elektronik posta gönderimi ve alımı uzak mesafelerdeki bilgisayarlar arasında dosya transferi gibi dönemin teknolojileri bakımından çok önemli yenilikler hayata geçmiştir. (Kırcova, 2005: 50-70).

Küreselleşen dünya, giderek karmaşıklaşan bilgi ve teknolojinin hüküm sürmeye başladığı bir köy haline gelmiştir. Bu küçük köyde bilgiyi elinde tutan ve işleyen, neredeyse tüm güce sahip olacak hale gelmiştir. Günümüzde neredeyse her haneye giren internet, bilgi fazlalığını üretmiştir. Buda bu bilginin işlenmesi ve güvence altına alınması gerekliliğini ortaya çıkarmıştır. Bilginin olduğu ve bilginin konuşulduğu yerde ise bir önemli konu, yani istihbarat ortaya çıkmaktadır.

Üretilen bilginin işlenmesi ve faydalın hale getirilmesi, istihbarat toplulukları açısından önemlidir. Toplumdaki iletişim ağını ve bilgi akışını izlemek, bu ağlardaki bilginin işlenmesi ve bu ağlardan faydalanmak istihba-

rat örgütleri açısından neredeyse bir adım öne geçmeyi sağlayan önemli bir noktadır. Toplumunu sosyal medya ve dijital alanda izlemek ve analiz etmek, olası yeni eğilimleri ortaya çıkarmak, tehditleri önceden tespit etmek ve bu Tespitler doğrultusunda güvenlik önlemleri almak Sosyal Medya İstihbaratının (SOCMINT) kavramını ortaya çıkarmıştır. SOMINT: İstihbarat örgütleri klasik istihbarat üretim sürecinde, bilgisayarın kullanımı ile önemli bir adım atmıştır, istihbarat çarkı açısından da önemli gelişmelere sebebiyet vermiştir (Lowenthal, 2008: 15-18). SOMINT'ın bir istihbarat disiplini olarak ortaya çıkmasıyla, istihbarat çarkı evrilmiş ve yakın zamanlı veri ve bunu işlenmesi, çalışan birimlere öngörü ve iç görü, suç unsurlarının tespitinin daha hızlı ve efektif bir hal almasıdır (Omand,2017: 350-370).

Dünya bir sosyal medya çağında yaşamaktadır. Facebook, Google, LinkedIn gibi kimlik bilgilerinin paylaşıldığı, insanların iş, arkadaş, sosyal paylaşım alanı bulmak için etkileşim kurmak istedikleri mecralar günümüzde artmakta ve artmaya devam edecektir. Facebook sosyal iletişim platformunun 2022'nin üçüncü çeyreği itibariyle aylık yaklaşık 2,96 milyar kullanıcısı olduğu belirtilmiştir (S. Dixon, 27 Eki 2022, Statica). Tüm dünya nüfusunun neredeyse yüzde 38'nin Facebook'a erişim sağlamaktadır. 1.968 milyar kişinin Facebook platformuna günde bir kere giriş yaptığı istatistikler ile de ortaya koyulmuştur (Meta Facebook raporu,2022). Sosyal medya ve dijital ağlar hayatlarımıza girdikçe kamusal alan genişlemekte ve dolası ile kamu kurumlarının ve devletlerin ilgisi bu alana yönelmektedir. Günümüzde sosyal medya ve dijital platformlar kamu güvenliği ile içi içe girmiş durumda ve güvenlik ve istihbaratın ana konusu haline gelmiştir. Hong Kong'ta yapılan denizcilik konferansında Somali ve çevresindeki korsanlarının Twitter'ı etkin kullandığı iddia edilmiştir. Gemi rotalarından, yüklenen yüke kadar korsanların tüm dünyadaki hesapları kontrol ettiği, ciddi araştırmalara yaptığını ve hedeflerini buna göre seçtiğine dair emareler olduğu iddia edilmiştir. İncelenen olayın ciddi güvenlik açığı olduğu ve dolası ile istihbarat ve örgütlerinin de ciddi ilişkisini çekmiştir (Diego Laje, CNN,2012).

Makale de ana araştırma konusu olan; Oyunlar üzerinden istihbarat, SOCMINT'in izleme ve değerlendirme sürecine dâhildir. Süreci izleyerek,

bilgilerin toplanması, doğrulanması ve analiz edilmesi olarak tanımlanmıştır (Norton-Taylor, R. The Guardian 2012). SOCMINT, aslıdan karar verme denkleminde bilinmeyenleri azaltma amaçlıdır. İnternet dünyasındaki avantajları arttırıp ve dezavantajları azaltmak amacıyla kullanılan SOCMINT, kanun ve kurallar çerçevesinden sanal alemde toplumu izlemek için kullanılmaktadır. Kimi zaman SOCMINT ile gruplar üzerinden davranış kalıpları oluşturulabilir. Güvenliğin bozulduğu dönemlerde, radikalleşen ve şiddete yönelen grupları izlemede ve bu grupları yönlendirmede kullanılır. Anlık güncellemeler ile her zaman güncel olmayı başaran SOCMINT anlık veri toplayarak dijital dünyayı yönlendirmeyi ve yönetmeyi kolaylaştırmaktadır (Omand, Bartlet and Miller, 2012: 810-825).

3. DİJİTAL OYUN VE MOBİL OYUN KAVRAMLARI

Oyun; TDK sözlük olarak, yetenek ve zekâ geliştirici, belli kuralları olan, iyi vakit geçirmeye yarayan eğlence olarak dilimizde tanımlanmaktadır. Dijital oyun, video oyunu olarak tanımladığımız yeni nesil oyun ise elektronik ortamlarda kişilerin karşılıklı olarak gelerek mücadele ettikleri ortamlara olarak günümüz dünyasında var olmuştur (Kent,2000: 83). Hızla Gelişen teknolojinin değişimi, internetin hayatımızda büyük önem taşıdığını ve her alanda kendini gösterdiği günümüzde insanların interneti kullanım amacının değiştiği ve farklılaştığı, bu kapsamda dijital oyunlarında oyuncular üzerinde algılama ve verdiği tepkilerin, kullanım amaçlarının değiştiği gözlenmektedir. Dijital oyunlar teknolojinin gelişen ve değişen algısıyla gerçek hayat ile sanal gerçekliğin birlikte sunulduğu günümüzde, sosyal hayatın bir parçası olarak hayatımıza birçok yerinde zaman geçirmemizin ötesinde getirdiği faydaların ve kolaylıkların yanı sıra, dijital oyun kullanımını bireysel ve toplumsal hayatımıza yönelik tehditler de barındırmaktadır. Dijital oyunların içerisinde oyun türlerine göre barındırdıkları sesler, görseller ve hareketler adeta gerçek ile bire bir aynı hazzı vermesi kullanıcılar arasında bağlılığı arttırdığı önemli faktörlerdendir.

Dijital oyunlar gerçek hayatın kopyalanarak kendisine özgü yansıtmasıyla dijital ortamda yeniden üretildiği yerlerdir. İnsan sürekli doğası gereği etkileşim içerisinde olduğu çevreye uyum sağlar. Dijital oyunlar kendi-

sine yansıtılan dijital ortama adapte olarak hızlı öğrenme sürecine girer ve kabullenir (Darıca,2013: 8-15). Uluslararası ticaretin kendini devamlı yenileyen ve değiştiren dijital oyun sektöründe son 15 yılda uluslararası ticarete önemli bir yer edinmiş ve sektör haline gelmiştir (Hünler,2021). Dijital oyun sektörü Uluslararası ticaretin yapı taşları olan enerji ve otomotiv sektörlerini geride bırakarak son zamanlarda hızla büyüyen bir evreye gelmiştir.

Dünyada yaşanan Covid-19 salgınının etkisi, akıllı telefon ve tablet teknolojilerindeki değişim, kullanım süreleri ve yerinin artması, bilgisayar ve oyun konsollarının üretim maliyetlerinin azalması ve kullanıcı görüntü yaşlarının genişlemesinin etkisi büyüktür (Dijital Oyunlar Raporu, 2019).

Dijital Oyun Pazarı hakkında en son trendler, önemli fırsatlar, itici güçler ve oyunun büyümesiyle ilgili zorluklara vurgu yapan bir rapor yayınlanmıştır. Raporda 2022-2031 yılları arasında Dijital Oyun Pazarının, öncelikle dünya çapında artan dijital oyun teknolojileri mal ve hizmet ticaretinde büyüme beklenmektedir. Dünya Bankası istatistiklerine göre, küresel olarak dijital oyun teknolojileri ihracatı 2017 yılında toplam mal ihracatının %11,64'ünü kapsamaktadır. 2019 yılında toplam mal ihracatının %11,53 olarak yükselmiştir. Mayıs 2021 yılında yayınlanan raporda, ABD Ekonomik Analiz ve İstatistik Bürosu, Mart 2021 yılı itibarı ile dijital oyun teknolojileri transferinde, Covid-19 salgını döneminden sonra ciddi derecede bir büyümeyi beklemektedir.

2022-2035 projeksiyonunda, Amerikan dijital oyun piyasasında ciddi bir genişleme tahmin edilmektedir. Veriler incelendiğinde Şubat 2021 teknoloji ihracatı 12,4 milyar dolar artarak 200 milyar dolara gelmiştir. Bu artış ciddi ve süregelen yükseliş trendi ile bu miktarlara gelmiştir. Yine dijital oyun piyasası verileri incelendiğinde, Şubat-Mart 2021 dönemi bir aylık sürecinde 20 milyar dolarlık ciddi bir artış gerçekleştirmiştir, bu da yılsonu genel ihracat rakamını 274 milyar dolar olarak gerçekleştireceği tahminin ortaya koymaktadır (Kenneth Araştırma, 2022).

Kullanılan sosyal iletişim araçları ve dijital oyunlar; zaman ve iletişim örgüsünün hızlı ve gerçek zamanlı olmasıyla kültürel, sosyolojik, psikolo-

jik, siyasi ve tarihi vb. etkileşimlerin yapıldığı yerlerdir. Gerçeklik algısının birebir yansıtıldığı dijital oyunlar oyuncu ile sunulan karakterin pozitif veya negatif şekilde bütünleşerek özdeşleşebilir. Her şeyden önce şiddet türündeki oyunlarda ödüllendirme sisteminin psikolojik birey davranış etkilerine göre yapılması dijital oyun ortamında oyuncunun farklı ruh haline bürünmesine yol açmaktadır. (Darıca, 2015: 15-20).

4. DİJİTAL OYUNLARIN BİREYİ ETKİLEME YÖNTEMLERİ İLE İSTİHBARAT ARASINDA Kİ İLİŞKİ

Dijital oyunlar, gerçek hayatta, bireyler için neredeyse imkânsız olan arzularını giderme ve kişisel benlik duygularını ön plana koymayı başarabildikleri bir alandır. Oyundaki birey kanunlarla sınırlandırılmış hayat içerisinde gündelik olarak imkânsız faaliyet ve davranışları rahatlıkla sergileyebilmekte ve iç dünyasını rahatlıkla dışarı yansıta bilmektedir. Adam öldürme, yaralama, mala zarar verme, hırsızlık gibi kanun dışı faaliyetlerin oyun alanında rahatlıkla gerçekleştirilebiliyor olması kimi analistler tarafından bireylerin kendisini bu şekilde dizginlediğini varsaysa da aslında bu bireylerin kişilik yapılarının hangi etmenler karşısında ortaya çıkabileceğinin en basit ölçme yöntemlerinden biridir (Huizinga,2017).

Dijital platformlar, şirketler tarafından oluşturulmuş sentetik dünyalardır ve bu oyun alanları teknolojik tasarım mekânları, hiçbir anlamda gerçek olmasa bile bireylerin saatlerce zamanlarını geçirecekleri ortamlardır (Telci,2013:783). Oyunlarda bireylere sunulan imkânlar ile çevrim içi şiddet olarak tanımlanan, bireylerin siber zorbalıktan araçsal şiddete kadar yer alan eylemleri, zamanla kendilerinde şiddet biçimini algılamasını da etkilediği ve değiştirdiği gözlemlenmiştir. Uzaktan ateş ederek bir bireyin oyunda öldürülmesi, şiddet olarak tanımlanmamıştır. Bu da algının ve mantığın nasıl etkilendiğinin bir örneğidir (Özçam, 2019: 105-110). Oyuncuların oyunları oynarken oyundaki karakter ile kendilerini özdeşleştirdikleri, hayal güçlerini kullanarak karakteri kendi hayat gerçekliklerine dönüştürdükleri, oyundaki başarısızlığın kendilerini olumsuz olarak etkilediği araştırmalarda ortaya çıkan sonuçlardan bir diğeridir (Yığıtoğlu,

2018: 195-215). Oyunların pazarlama yöntemlerinden biriside sosyalleşmeyi sağladığı yönündedir. Oyuncular oyun içerisinde farkında olmadan oyun dışındaki farklı konulardan rahatlıkla bahseder, konuşurlar. Oyuncular birbirleri arasında bu şekilde kalıcı ve bağ oluşturabilmektedir. Buda oyunun motivasyonu olarak tanımlanmaktadır (Bartle, 1996: 12-18). Kitle iletişiminin yoğun yaşandığı günümüzde, üretilen iletişim araçları gerçeklik ile akıl arasında bir ilişki kurarak akıllardan bilgi çalabilmektedir. Kitlelerin bulunduğu ortak alanda ortaya çıkan bilgi, oluşturulan sayısal alan rahatlıkla yayılmaktadır. Tüm kullanıcıların dâhil olduğu bu enformasyon akışında bilgi kirliliği ile akıl oyalanması da gerçekleştirilebilmektedir.

Bu akıl bulanıklıklarının orta çıktığı dijital oyun platformlarının yarattıkları olumsuz etki çevremizde varlığını sürdürmektedir. Küresel dünyada pazarlama teknikleri kullanılarak sunulan bu oyunlar, güzelliklerinin arkasında akılı yoran ve bireyi boşlukta hissetmesini sağlayan bir karanlık oluşturabilmektedir. Çünkü zamanla gerçeklik ile sanal arasındaki farkı algılamayı bırakan akıl, oyun oynanmadığı saatlerde bile oyun ile meşgul olmakta, bireyin oyundan çıkması tam manasıyla mümkün olmamaktadır. Akıl, bu algoritmik yapısı tasarlayan birey-kişi ya da kurumların kurguladığı dünya içerisinde kendini bulmaya çalışmakta, farkında olmadan yönlendirmeler ile kendini bulmaya çalışmaktadır. Zamanla ortaya çıkan bu akıl bunalmaları bireyi mahveder ve hakikatten uzaklaştırır. Narkoz etkisi yaratarak zamanla hakikatlerin algılanmasına bile engel olabilir (Yarrar, 2019: 110-125).

Küresel sistem içerisinde her alanda faaliyet yürüten devlet ve istihbarat teşkilatlarının verdikleri destekler ile çektikleri sinema filmleri ile toplumu yönlendirme, bilinçaltı mesaj, gerçeği yalandan yalanı ise gerçekten soyutlayarak propaganda yaptığı önceden öngörülemeyen ancak yayınladıkları sahneler ile toplumu bazı durumlara hazırladıkları görülmektedir. Dijital oyunlar ise yeni bir kavram tarzıyla farklı şekil ve türlerde sinema filmlerine benzer mesajlar vermektedir. İstihbarat anlamında dijital oyun piyasası ele alındığında internet kullanarak çevrimiçi oynanması ve internet bağlantısına gerek olmadan offline oynanması ayrımı bulunmaktadır. Bilgisayar ve

bileşenleri kullanarak arttırılmış gerçeklik veya sanal gerçeklik sayesinde oyun konsolları aracılığı ile offline oynanan oyunlar verilen ve yapılmak istenen hareket ve görevlerle içerik olarak birtakım bilgiler vermektedir. Offline oynanan oyunlar internete bağlanarak oynanması halinde oyuncular/kullanıcılar arasında sesli iletişim yapmak suretiyle haberleşmeyi sağlamaktadır. Bu yapılan haberleşmeler oyun geliştiricisi veya diğer çeşitli veri merkezleri tarafından kaydedilmektedir (Tırnovalı,2019).

Rusya ABD ile uzun yıllardan beri mücadele etmektedir. Dijital dünya, soğuk savaş döneminden sonra konvansiyonel silah ve istihbarat yöntemlerinin yerini almıştır. Her ne kadar yapılan bu mücadeleler ve müdahaleler Rusya tarafından kabul edilmese de dijital izler Rusya'nın bu kulvardaki varlığını ortaya koymaktadır. Beyaz saray ve NATO'ya yapılan müdahalelerin arkasında Rusya devletinin olduğu ABD tarafından her zaman dillendirilmektedir. 2007 yılında Estonya, Rusya'yı siber savaş başlatmak ile suçlamıştır (Traynor,2007).

2020 yılında dönemin ABD Dışişleri Bakanı Mike Pompeo, Enerji Bakanlığı Ulusal Nükleer Güvenlik İdaresi de dâhil olmak üzere hükümetin büyük bir kesiminde bildirilen izinsiz girişlerin olduğunu, iç güvenlik bakanlığının konuyu araştırdığını söylemiş ve olayla ilgili olarak Rusya'yı suçlamıştır (Johnson ve Snider,2020). Saldırıyı inceleyen uzmanlar 21 yy. da casusluğun özel şirketler üzerinden bilgisayar sistemleri üzerinden yapılmaya başladığını belirtmiştir.

Baltimore merkezli bir siber güvenlik firması olan ZeroFOX'un küresel güvenlik mimarisi ve tehdit istihbaratı başkanı Ross Rustici, “Şu anda tüm ülkelerin oynadığı bir zamanlar analog casus oyunlarının dijital devamına tanık oluyoruz” demiştir (Snider ve Guynn,2020). Ülke dışarısında bu gibi ithamlarla karşı karşıya kalan Rusya Devleti çevrimiçi oyunlara yönelik bir kanun yürürlüğe koymuştur. Teröristlerin çevrimiçi oyunlar üzerinden haberleştiklerini belirten yetkililer, FSB (Terörle Mücadele Kanunu) çevrimiçi oyun ve sosyal ağlardaki kullanıcıların kimliklerinin tanıtılması şartını koymuştur. Bilgi Teknolojileri ve Bilgilerin Korunması Hakkında” kanunda yapılan düzenlemede, FSB'nin talebi üzerine kullanıcı yazışma-

rı ve şifreleme anahtarları, kullanıcıların cep telefonu numaraları FSB' ye verilecektir. (<https://www.rbc.ru>,2017), (pravo.gov.ru,2017).

Siber mücadeleler yaşanırken. ABD Eski Ulusal Güvenlik Ajansı yüklenicisi Edward J.Snowden, İstihbarat uzmanlarının çeşitli dijital platformlardaki çevrimiçi oyunlara sızdığını, milyonlarca insanın verilerini topladıklarını açıklamıştır. Sahte karakterler yaratarak, oyunlara sızdıklarını, burada oyuncular ile iletişime geçerek verileri alıp, bu verileri analiz ettiklerini, bu şekilde gözetleme, muhbir elemanı gibi personelleri buralardan seçerek işe aldıklarını belgelerle açıklamıştır. Özellikle ABD ve İngiliz istihbaratının bunu kullandığını, zararsız olarak görülen çevrimiçi oyunların göz önünde saklanmanın bir yolu olduğunu belirtmiştir (Mazetti ve Elliot, 2013). NSA ajanı Snowden'in yaptığı ifşaatlar arasında önemli bir rapor bulunmaktadır. Rapor "Games: A Look At Emerging Trends, Uses, Threats And Opportunities In Influence Activitive" adıyla web sitelerinde dolaşıma sokulmuştur. Raporda oyunlar üzerinde daha sonra bahsedeceğimiz gibi önemli verilerin elde edildiği belirtilmektedir. Raporda: oyun alanı, teröristleri tespit etmek için potansiyel fırsatlar sunar, sanal ekonomilerdeki para akışını izleyerek finansal operasyonlar ve sanal ürünlerin alım satımına ve bağış toplamaya kimin dâhil olduğunu belirler demektedir. Burada SAIC Prototipini kullanarak terörist oyun trendlerini takip etme gibi noktalar ön plana çıkarılmıştır. SAIC'in terörist Web sitesi içeriğini otomatik işleme yeteneği, terörist çevrimiçi oyunları izlemek için benzersiz bir fırsat sağlar. Veri işleme ve raporlama şunları ele alabilir: (1) mevcut popüler çevrimiçi oyunlar ve ilgili söylem, (2) bu topluluklarda ortaya çıkan sosyal ağlar, (3) popüleritesi artan veya azalan oyun ve topluluk siteleri, (4) yeni siber uzaydaki terörist oyun siteleri veya değiştirilmiş güncel oyun siteleri, (5) terörist oyun faaliyetinin çevrimiçi yayılması ve (6) terörist oyunlar hakkında materyal barındıran web siteleri" konusunda bilgi verilmekte ve terörist organizasyonların istihbarat örgütleri tarafından izlendiği ve oyunların bu örgütleri izlediği belirtilmektedir.

Terör örgütlerinin çekirdek kitleye ulaşması ve hedef kitlesini hedeflemesi için internete benzer güçlü bir ortam yaratarak daha olgun ve genişletilmiş bir oyun alanının etkileştirici olacağı, oyun içinde istihbarat

personelini sızması ve bu personel ile oyun alanındaki önemli propaganda çabalarının tespit edilmesinin de sağlanacağı raporda belirtilmektedir. Propagandanın tanımlanması, oyun üreticisiyle birlikte çalışarak zararlı veya yanıltıcı bilgilerin oyun alanından çıkarılmasına ve/veya bir karşı propaganda kampanyası geliştirilmesine olanak tanıyacağı cümlesinden de oyun üreticisi ile çalışıldığı anlaşılmaktadır (NSA,2007,8-10, Chapter Addendum 69-70).

Bu kulvarda önemli aktörlerden birisi de Çin devletidir. 2019 yılında yayımlanan bir raporda, FBI raporlarına dayandırılarak APT 41 GROUP(<https://www.fbi.gov>,2021) adlı Çin devleti bağlantılı bir bilgisayar korsan grubunun varlığından söz edilmektedir. Grubun çevrimiçi oyun ağlarına saldırı düzenleyerek bilgi çaldıkları, 2014'ten beri Çin için stratejik istihbarat sağladıklarını belirtilmektedir (Palmer,2019). Ülke dışında bu gibi faaliyetler yürüttü iddia edilen Çin, ülke içerisinde oyunlar üzerinden olası sızmaları engellemek için ağır önlemler uygulamaktadır. Çin yasaları, Batılı yayıncıların Çin'in büyük ve büyüyen oyun pazarına erişim sağlamak için Tencent ve NetEase gibi Çinli şirketlerle ortaklıklar kurması gerektirmektedir. Bu sayede oyunlar denetlenmekte ve oyun içermesinde olası bir sızmaya devlet üzerinden müdahale edilebilmektedir (Aitel ve Schneider, 2020).

5. GÜNÜMÜZDE ŞİRKET VE DEVLET İSTİHBARAT ÖRGÜTLERİNDEKİ ETKİLEŞİM

Yeni dünya düzeninde ülkelerin savaşlarda özel şirketleri kullandığı, bu değişen ve gelişen asimetrik olgunun istihbarat faaliyetlerinde de hissedildiği, devletlerin istihbarat teşkilatlarından ziyade özel şirketler yoluyla bu faaliyetleri gerçekleştirdikleri bilinmektedir. Günümüzde ülkemizi ve dünya basın ve yayın organlarını meşgul eden Pegasus casus yazılımı buna örnek teşkil edebilir. İsrail'in en bilinen siber casusluk ve teknoloji şirketi olan NSO Grup, 2010 yılında Herzliya kentinde üç İsraili tarafından kurulmuştur. NSO, İsrail askeri istihbarat servisi AMAN' DA teknik istihbarat faaliyetlerinde temel rolü olan Unit 8200 teşkilatından gelen üç kişi

tarafından kurulmuştur (Çahmutoğlu,2021). Savunma sanayi sektörü gibi stratejik siber teknoloji şirketleri de ürünlerini diğer devletlere satabilmesi için Savunma Bakanlığının ve ilgili kuruluşların onayı gerekmektedir. Üretilen ve geliştirilen ürünlerin pazara hâkimiyeti, ikamesinin olmaması stratejik olarak mevcut üretici ülkenin diğer ülkelerle ilişkilerini kendisinin belirleyeceği ve elinde koz olarak kullanacağı hale getirmektedir.

Devlet İstihbarat birimleri kendi içerisinde geleceğe yön veren veri analizini yapay zekâ üzerinden yapabilen teknoloji şirketleriyle ortak çalışmaktadır. İngiltere, istihbarat servisleri MI5, MI6 ve GCHQ'nun verilerini depolaması için Amazon ile 1 Milyar Sterlin değerinde sözleşme imzalamıştır (Syal,2021). İstihbarat örgütlerinin görünürde veri depolaması olarak yapılan anlaşmaları arkasında bu şirketlerin veri depolarını da kullandığı, şirketlerin kendi ulaşılabilirlikleri sayesinde rahatlık veri analizi yapabildikleri hem de hedefe rahatlıkla ulaşabilecekleri iddia edilmektedir.

2022 yılı ilk çeyreğinde Rusya ile Ukrayna arasında güvenikleştirme çerçevesinde yapılan ve gerek konvansiyonel gerek Hibrit teknolojilerinin tümünü kullanılarak, tüm siber çerçevede bu mücadelesinin yayılması, Ukrayna'nın teknoloji açısından da yürüttüğü savaşın göstergesidir. Ukrayna Başbakan Yardımcısı ve Ukrayna Dijital Dönüşüm Başkanı Mykhailo Fedorov, öncelikli olarak Twitter olmak üzere tüm dijital platformlar üzerinden mücadeleye başlamış, tüm dünyayı Twitter üzerinden Ukrayna'daki olaylara dikkati çekmesini sağlamıştır. Olayların başladığı şubat ayından itibaren bütün dijital platformlarla iletişime geçip, platformların Rusya da faaliyetlerini durdurmaya çağırılmış, çağırısına birçok şirket olumlu cevap vermiştir. Bu olay günümüzde sanal dünyada ki iki ülke savaşının en önemlisi sayılabilir (Federov,2022, Twitter).

Makalenin ana alanı olan dijital oyunlar üzerinden istihbarat faaliyetleri konusu özelinde, dijital mobil oyunlarının Pegasus casus yazılımı gibi uzaktan erişim sağlayabilen uygulamalara izin verip vermediği teknik olarak ispatlanmış bir alan değildir. Lakin bunun ispatlanmasının da mümkün görülmemektedir. Neredeyse yapılan yaşadığımız yüzyılın başında ki istihbarat faaliyetleri 50 veya 100 yıl sonra devletler tarafından akademik çalışmalara açılan arşivlerden ancak anlaşılabilir. Bu sebeple bulun-

duğumuz dönemde yapılan ve adı geçen faaliyetlerin ispatlanabilmesi belki gelecekte açıklanacak arşivlerle günümüze ışık tutacaktır.

6. MOBİL APP -ON LİNE OYUN PİYASASI- ÜRETİCİ-DEVLET İLİŞKİSİ

Oyun firmaları ve üreticilerin incelenmesi zorunluluğu önemlidir. Oyun piyasaları her geçen gün gelişmekte ve ekonomik bir alanda genişlemektedir. 2022 Nisan ayı verilerine göre 7,93 milyar dolarlık bir ekonomik genişliğe sahip olan dijital oyun piyasası, 5 milyar insanın kullandığı internet dünyasında, günde 5 saatlik bir ortalama zaman geçirme süresine sahiptir. Bu 5 saatlik zamanı internette geçiren kullanıcıların yüzde 50'si mobil araçları ile internete bağlanmakta ve bu mobil cihazları ile oyun oynamaktadır (Gök ve Ünal,2022: 160-163).

a) Strateji Oyunları ve Üretici-Devlet ilişkisi

Strateji oyunları, mobil oyun piyasasında en çok tercih edilen oyunlardandır. Özellikle gençler arasında ilk sıralarda yer almaktadır. Bu sebeple strateji oyun yazılımcı firmaları incelemek, oyunlar üzerindeki kontrol hangi merkezden yapıldığını bir noktada yön verecektir.

Online Aplikasyon mağazalarında Strateji alanında ilk on şirket incelendiğinde Çin'in önemli bir ağırlığı görülmektedir. Her ne kadar ticari şirket olarak bu pazarda yer alsada bu şirketlerin birçoğunun arka planında Çin devleti ile bilgi paylaştığı göz önünde bulundurulması gereken bir noktadır. Tabloda birinci sırada yer alan İGG Çin asıllı bir firma olmasına rağmen merkez olarak Singapur'u göstermekte ve Hong Kong'da işlem yürüttüğünü belirtmektedir. Listede beşinci sırada yer alan TopwareStudio şirketi 1996 yılından beri Almanya'da hizmet vermektedir. ABD'de TopWare Interactive Inc. Aynı şekilde strateji oyunu üreticisi olan ve sürekli mahkemelik olduğu bir şirket mevcuttur (Golem.de, 2005). Listede yer alan şirketlerin internet siteleri incelendiğinde Orta Doğu'yu hedefleyen Çin devlet destekli bir şirket olduğu görülmektedir.

Tablo 1: Strateji Oyunu Pazarı (<https://42matters.com>)

OYUN ADI	YAYINCISI	ÜLKE	İNDİRİLME SAYISI	WEB SİTESİ
Lords Mobile: Krallık Savaşları	IGG.COM	ÇİN	100.000.000+indirme	https://www.igg.com/
State of Survival: TheWalking Dead İşbirliği	Kings Group Holdings		50.000.000+ indirme	https://www.sosgame.co.kr/
Mafya Şehri	YottaGame	ABD	50.000.000+ indirme	http://www.longtech.hk/
Klan çatışması Top War: Battle Game	Supercell Topwar Studio	FİNLANDİYA ALMANYA	500.000.000+indirme 10.000.000+ indirme	https://supercell.com/en/ https://www.topware.com/
Rise of Kingdoms: LostCrusade Days of Empire - Kahramanlar Asla Ölmez!	Lilith Games	ÇİN	10.000.000+ indirme	https://www.lilithgames.com/
Rise of Empires: Iceand Fire	ONEMT	ÇİN	5.000.000+ indirme	https://www.onemt.com/
TheWalkingDead: Hayatta Kalanlar	LongTech Network Limited Galaxy Play Technology Limited	ÇİN	10.000.000+ indirme 1.000.000+ indirme	http://www.longtech.hk/ http://galaxyplay-tech.com/
Avalon Kralı: Hâkimiyet	Century Games Limited	ÇİN	50.000.000+ indirme	http://www.funplus.com/

b) Simülasyon Oyunları ve Üretici-Devlet ilişkisi

Mobil oyun piyasalarında önemli bir oyun pazarı ise Simülasyon oyunlarıdır. ABD ordusunun benzetim, personelini **eğitmek** için kullandığı bilinmektedir. Multi-purpose Arcade Combat Simulator (Super Nintendo), Virtual Reality Combat Training, Full Spectrum Warrior (Xbox), Tactical Iraqi (PC), America's Army (PC, Xbox) gibi oyunlar aslında personeli **eğitmek için çıkarılmış** ve firmalar tarafından ticari öğeye dönüştürterek piyasa sunulmuştur. Bu oyunların sahadaki kullanıcı geri dönüş verileri incelenerek oyunlarda yükseltmeler yapıp askeri modellemelerde uygulandığı bilinmektedir. (Stilwell, 2016: 1). Simülasyon oyunlarında birçok şirket listede yer almaya çalışmaktadır. Genel olarak ilgi çekici ve zaman geçirme açısından uzun zaman ve akıl kullanma açısından çok emek gerektirmeyen bu oyunlarda Çin ve Rusya yine ağırlığını göstermektedir. Pazarda birinci olan Ten SquareGames Polonyalı bir şirket olup 129 milyon EUR (153

milyon USD) 2020 yılı itibari ile gelir elde etmiştir (Partleton,2021). Listede yer alan Tamadog-LiftApp LLC oyunun sitesi incelendiğinde site kendisini <https://www.appsyoullove.com/> adresine yönlendirilmektedir. Site içeriğinde ve gerek web’de yapılan taramalarda açık bir bilgi bulunmamaktadır. Sitenin geliştiricileri konusunda araştırma yapıldığında ise sitenin gerçek sahibine ulaşılamamaktadır. Bu da akıllarda soru işareti oluşturan dikkat çekici bir noktadır. Oyun piyasasında ki veriler değişen bir yapıya sahip olmasından dolayı web sitelerin içerikler değişebilmektedir.

Tablo 2: Simülasyon Oyunu Pazarı (<https://42matters.com>)

OYUN ADI	YAYINCISI	ÜLKE	İNDİRİLME SAYISI	WEB SİTESİ
Balıkçılık Clash	Ten Square Games	POLONYA	50.000.000+ indirme	https://tensquaregames.com/
Otobüs Simülatörü: Ultimate	Zuuks Games	TÜRKİYE	50.000.000+ indirme	https://www.zuuks.com/
LUV - İnteraktif Oyun	Afivad Limited		1.000.000+ indirme	
Klondike Maceraları	VizorApps Ltd.	BİRLEŞİK KRALLIKLAR	10.000.000+ indirme	https://vizor-interactive.com/en/
Ejderha şehri	Socialpoint	İSPANYA	100.000.000+indirme	https://www.socialpoint.es/
Kedim: Sanal Hayvanım Tamagotchi Evcil Hayvan Simülatörü	Liftapp LLC	RUSYA	10.000.000+ indirme	https://www.appsyoullove.com/
AvatarLife - Sanal Dünyada Eğlence, Aşk Ve Oyunlar!	101xp Limited	ÇİN	10.000.000+ indirme	https://tr.101xp.com/
Boşta Mafya- İş Adamı Yöneticisi	Century Games Pte.	ÇİN	5.000.000+ indirme	http://www.funplus.com/
Tamadog - Konuşan Köpek Oyunum (AR)	Liftapp LLC	RUSYA	1.000.000+ indirme	https://www.appsyoullove.com/
Sanal evcil hayvan				
SimCityBuildIt	ElectronicArts	ABD	100.000.000+indirme	https://www.ea.com/

c) Aksiyon Oyunları ve Üretici-Devlet ilişkisi

Aksiyon oyunları makalemizde belirttiğimiz gibi, gençlerin tercih ettiği bir diğer oyun türüdür. “MMO” türü “MMOFPS” veya “MMORPG” gibi isimler alabilmektedir. “MMOFPS” kitlesel çevrimiçi birinci şahıs aksiyon oyunları, bireylerin rol yapma ve bu gündelik hayatlarındaki psikolojik eksikliklerini kimi zaman tamamlamaya çalıştıkları bir hal alabilmektedir (Demirbaş, 2015: 21). Yapılan araştırmalarda kadın bireylerin aksiyon oyunlarını daha çok tercih ettikleri önemli bir veridir (Kars, 2010: 46).

Aksiyon oyunlarında da diğer oyun piyasalarındaki gibi Çin ve Rusya'nın önemli bir ağırlığı bulunmaktadır. Çin şirketlerini incelediğimizde Tencent ismi ön plana çıkan isimdir. Şirketin kurucusu (MaHuateng, 马化腾), Çin'in önemli milyarderlerinden birisidir (Eliot,2014). Çin Ulusal Halk kongresi Delegatesi olan Huateng, WeChat (Weixin) uygulamasının da sahibidir. Bu uygulama günümüzde Çin'in tamamında ve Dünya'nın yüzde 48'lik bir bölümünde kullanılmaktadır (Dolan,2017).

Tablo 3: Aksiyon Oyunu Pazarı (<https://42matters.com>)

OYUN ADI	YAYINCISI	ÜLKE	İNDİRİLME SAYISI	WEB SİTESİ
PubgMobile - Yeni Harita Karakın	Tencent Games	ÇİN	100.000.000+ indirme	http://www.tencent.com/
GarenaFreeFire - Dünya Serisi	GarenaInternational I PrivateLimited	ÇİN	500.000.000+ indirme	https://www.garena.sg/ https://www.activision.com/
Call of Duty: Mobile- Tokyo Escape	Activision Publishing, Inc	ABD	100.000.000+ indirme	https://supercell.com/en/ https://www.moonton.com
Kavga yıldızları	Supercell	FİNLANDİYA	100.000.000+ indirme	https://www.axlebolt.com/ http://www.tencent.com/
Mobil Efsaneler: BangBang	Moonton	ÇİN	100.000.000+ indirme	https://www.kabam.com/
Standoff 2	AXLEBOLT LTD	RUS	50.000.000+ indirme	https://www.kabam.com/
PubgMobileLite	Tencent Games	ÇİN	100.000.000+ indirme	https://www.kabam.com/
Marvel Şampiyonlar Turnuvası	Kabam Games, Inc.	KANADA	100.000.000+ indirme	https://www.kabam.com/
Savaş Makineleri: Tank Savaşı- Ordu ve Askeri Oyunlar	Fun Games ForFree		100.000.000+ indirme	
Savaş Robotları. 6v6 Taktiksel Çok Oyunculu Savaşlar	PIXONIC	RUS	50.000.000+ indirme	https://pixonice.com/ru

SONUÇ

Online olarak stratejik ve benzetim temelli oyunlarda, kullanıcıların verdikleri tepkiler ile stratejik olarak zekâ ve diğer arkadaşları ile iletişim kurarak yönlendirme, organize etme kabiliyetlerinin öğrenmek açısında bu bilgiler çok değerli görülmektedir. Sanal dünya, oyuncuların gerçek dünyada yapmalarına izin verilmeyen şeyleri yapmalarına izin verir. Bu gerçek MMORPG'lere de yansımıştır. Örneğin biri başka bir oyuncunun karakteri tarafından saldırıya uğradığında, bu kurban arkadaşlarından yardım isteyebilir. Arkadaşlar intikam almak için karşı koyabilir, saldırabilir veya suçlunun sanal mülkünü ve hatta nakit parasını soyabilir, bunların hepsi doğal kabul edilir. Gençler için çevrimiçi oyunlar, gerçek dünyada yapma-

ya cesaret edemeyecekleri şeyleri yapmalarına olanak tanır. Oyuncuların çoğu gençtir ve kendilerini kontrol etme yeteneğinden yoksundurlar ve akranlarından kolayca etkilenirler. Bu anti-sosyal ve cezai yönlerin yanı sıra, çevrimiçi oyun etkinlikleriyle ilgili birçok başka olumsuz sorun ortaya çıkarır. Oyun içerisinde kredi kartı ile oyunda alışveriş yapması durumunda kullanıcının gerçek kimliğine ulaşılabilir. Dijital oyunlarda kaydedilmiş veriler analiz yapıldığında dünyada ve ülkelerinde zekâ seviyesi yüksek insan kaynağı havuzu oluşturduğu ve eleman teminini bu havuzdan yapabileceği değerlendirilmektedir. Ayrıca dijital oyunlara ilk girişte verilen konum, mikrofon, kamera, fotoğraf galerisi, sosyal medya hesapları ve bunlara bağlı arkadaş ve takipçileri, telefon numarası, rehber, sms ve e-posta hesaplarına verdiği erişim izinleri gibi kişisel bilgilerinde istihbarat birimleri tarafından bu havuzda toplandığı ve işlendiği görülmektedir.

Askeri ve sivil kavram, sosyal, fen ve sağlık sektörünün oyunlaştırıldığı günümüzde, dijital oyunların kapsamının eğlence ve oyun altında incelenmesinin daha çok ötesine geçmiştir. Ülkemizin mevcut nüfus yapısı ve sosyal hareketliliği göz önünde bulundurularak oyunlar üzerinden toplanan veriler ülkemiz hakkında çok önemli projeksiyonlar oluşturulmasını sağlayabilmektedir. Bu olası toplanan verilerin kimler ve hangi grupların elinde olduğu konusunda, uluslararası güvenlik ve ülke güvenliği açısından da önem arz etmektedir. Terör örgütleri Türkiye’de geçmiş dönemlerde gerek sosyal platformlar gerek oyunlar üzerinden iletişim ağlarını kurmuş, yurt dışında ki bağlantıları ile iletişimlerini bu platformlar üzerinden sağladıkları ortaya çıkmıştır. Gelecekte böyle bir güvenlik ve istihbarat açığının oluşmaması için kurum ve kuruluşların bu konuda yetkinliğe sahip olması gerekmektedir. Dijital oyun bulut teknolojileri alanında veri toplama ve analiz merkezlerinin oluşturulması geleceğe yönelik atılan önemli bir adım olacaktır.

Olayın ekonomik yönden de önemli etkileri bulunmaktadır. Dijital oyun piyasası son 15 yılda dünyayı etkisi altına almıştır. Koronavirüs sebebiyle de geçtiğimiz bir buçuk yıl içerisinde büyük bir atağa kalkmıştır. Böylece ekonominin gözdesi olan sektörleri bile gerisinde bıraktığı gözlen-

mektir. Lakin Türkiye dijital oyun sektöründe yeteri kadar yerini alamadığı gözlenmektedir.

Dijital oyunlar üzerinde inceleme yapabilmek için, teknik yeterlilik ve ileri uzmanlık, eğitim gerektiren bir konudur. Mühendislik, Sosyoloji, Ekonomi, Güvenlik, İstihbarat konularında yetkinlik kazanan bireyler gereklidir. Vatandaşların güvenini ve emniyetini, korumak ve kollamak dehetin en temel görevidir. (Acar& Urhal, 2007: 76-77). Bu sebeple kamu güvenliği toplumsal açıdan her zaman devletin ilgilenmesi ve ihtimam göstermesi gereken bir konudur. Kamu güvenliğinin gençleri koruması gerekliliği ön plana tutulduğunda istihbarat örgütlerinin ve devletin en temel olduğu olan gençleri korumak her alanda gereklidir. Bu sebeple dijital dünyada da gençlerin korunması ve sınırların korunması kadar önemli bir noktadır. Makalemizde de bahsettiğimiz sosyolojik, psikolojik, mekânsal alana kadar yapılan istihbarat faaliyetlerinin farkına varılması için eğitilmiş ve teknik personel ile ileri teknik imkanlar gerektirmektedir. Ülkemizde yüksek eğitimden başlayarak bu hususa önem vermiştir.

2021 yılına ait Yüksek Öğretim Kurumu verileri incelendiğinde 4 yıllık lisans eğitimi veren Dijital Oyun Tasarımı bölümünün bulunmaktadır. Üniversitelerin İstinye, İstanbul Aydın, Beykent, Nişantaşı, Doğu, Beykoz, Bahçeşehir, Muğla Sıtkı Koçman, Doğu, İstanbul Ayrınsaray, İstanbul Bilgi, Doğu Akdeniz ve Arkin Yaratıcı Sanatlar ve Tasarım Üniversiteleri'nde eğitim öğretime devam ettikleri toplam 544 kontenjan miktarından 445 öğrencinin bölüme yerleştiği verilerine ulaşılmaktadır (YÖK,2022).

Millî Eğitim Bakanlığı yükseköğretim kurumları ile diğer kurum ve kuruluşların ihtiyaç duyduğu nitelikli insan gücünü yetiştirmek amacıyla 1416 sayılı kanun kapsamında YLSY bursu ile lisansüstü eğitim kapsamında yurt dışına öğrenci gönderilmesi ile ilgili 2021 yılı verileri incelenmiştir. 5 öğrencinin dijital oyun kapsamında dış ülkelere gönderildiği tespit edilmiştir (MEB YLS sonuçları 2021). Yurtdışına gönderilen ve yetiştirilen lisans mezunu statüsündeki yetkin kişilikler ile dijital oyun pazarına yönelik bir strateji planı belirlemeli ve ulusal güvenlik açısından bu planlar eş güdümlü bir şekilde uygulamaya konulmalıdır Az da olsa bu sayının

çoğaltılması önemlidir. Kendi dijital oyun yazılımlarının üretilmesi gerek ekonomik gerekse güvenlik açısından önem arz etmektedir.

Bu sebeple bu eğitim yatırımlarının ve bu konuda bireylerin sayısının arttırılması önem arz etmektedir. Dijital oyun ekonomik olarak geçmişte yaşanan krizlerde yoğun etkilenen diğer sektörler gibi mali krizlerden yoğun etkilenen bir yapıda değildir. Dünyadaki eski ekonomik yapılar değişirken ve yavaşlarken dijital oyun sektörü durmadan gelişmekte ve ekonomik alanını geliştirmektedir. Yeterli yatırım ve destek sağlanması durumunda, genç nüfusun istihdam sağlayabilecek potansiyelin olduğu da öngörülmektedir.

Kaynakça

Acar, Ünal ve Urhal, Ömer. (2007). *Devlet Güvenliği İstihbarat ve Terörizm*, Adalet Yayınları: Ankara.

Akyürek, Hüseyin Aziz. (2019). *İstihbarat Savaşları, Birinci Dünya Savaşında Suriye ve Lübnan'da casusluk faaliyetleri*, Yayına Hazırlayan, Polat Safi, Kronik 2019: İstanbul.

Altheide, David L. (2004). *The Control Narrative of the Internet, Symbolic Interaction*, Volume 27, Number 2, p. 223–245.

Aitel Dave and Schneider Jordan. (2020). *If You Play Videogames, China May Be Spying on You*, October 28.2020, <https://www.wsj.com/articles/if-you-play-videogames-china-may-be-spying-on-you-11603926979>.

Bartle, Richard Hearts. (1996). Clubs, Diamonds, Spades: Players Who Suit Muds. *Journal of MUD Research* 1.1.1996 1-19. <http://mud.co.uk/richard/hcds.htm>.

Çahmutoğlu, Ersin. (2021). Dünyayı tehdit eden casus yazılım: Pegasus. <https://www.aa.com.tr/tr/analiz/dunyayi-tehdit-eden-casus-yazilim-pegasus/2314321>

Chen Ying-Chieh; Patrick S. Chen and Ronggong Song. (2004). Online Gaming Crime and Security Issue. Cases and Countermeasures from Taiwan, The 2nd Annual Conference on Privacy, Security and Trust (PST'2004), October 13-15, 2004, Fredericton, New Brunswick, Canada.

Darıca, Sefer. (2015). *Dijital Oyunlarda Kullanılan Subliminal Mesajların Gerçeklik Algısı Üzerindeki Etkilerine Yönelik Bir Çalışma: Gerçeklik Eşiği Kavramı*. *Turkish Studies International Periodical for the Languages, Literature and History of Turkish or Turkic* Volume 10/14 Fall 2015, p. 181-202 DOI Number, <http://dx.doi.org/10.7827/TurkishStudies.8778> ISSN: 1308-2140.

David, Omand. *“Social Media Intelligence: SOCMINT”*, The Palgrave Handbook of Security, Risk.

Delibalta, Yavuz. (2018). *Selçukluda İstihbarat*, Yeditepe Yayın Evi: İstanbul.

Demirbaş, Kerem Yavuz. (2015). *Dijital Oyunlara “oyun türü” yaklaşımlarının Sorunları: “platform oyunları” türü örneği*. Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi-, 9 (1): s.363-387 Ağustos 2015: Konya.

Devlin, Sam. vd. (2014). “*Game intelligence*,” 2014 IEEE Conference on Computational Intelligence and Games: Dortmund, Germany.

Dickey, Michelle. D. (2004). Game design narrative for learning: Appropriating adventure game design narrative devices and techniques for the design of interactive learning environments. *Educational Technology Research & Development*, 54, s.245–263.

Diego, Laje. (2012). *#Korsan? Modern korsanları Twitter üzerinden takip etme*, <http://edition.cnn.com/2012/03/15/business/somalia-piracy-twitter/index.html> Erişim Tarihi: (05.10.2022). *Dijital Oyunlar Raporu*. (2019). Güvenli İnternet Merkezi, <https://www.guvenliweb.org.tr/>

Dolan, Kerry. (2017). Chinese Billionaire Behind Tencent Briefly Richer Than The Google Founders, <https://www.forbes.com/sites/kerryadolan/2017/11/21/chinese-billionaire-behind-tencent-cracks-the-worlds-top-ten-richest-for-the-first-time/?sh=75747e71446e>

Dover, Robert; Dylan Huw and Goodman Michael S. (2017). *The Palgrave Handbook of Security, Risk and Intelligence*, (London: Palgrave Macmillan, Palgrave Macmillan; 1st ed. 2017 edition. Dixon, Stephan. 27 Eki. 2022. <https://www.statista.com/statistics/264810/number-of-monthly-activeFacebookusersworldwide/#:~:text=With%20roughly%202.96%20billion%20monthly,years%20to%20reach%20this%20milestone>.

Elliott, Dorinda (2014), Tencent the secretive, chinese tech giant that can rival Facebook and Amazon, <https://www.fast-company.com>-Fidan, Hakan. (1999). *Intelligence And Foreign Policy: A Comparison Of British, American And Turkish Intelligence Systems*, Yüksek Lisans Tezi, Bilkent Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara, Türkiye.

Glassman, Michael and Kang Min Ju. (2012). Intelligence in the internet age: The emergence and evolution of Open-Source Intelligence (OSINT), Computers in Human Behavior Volume 28, Issue 2, March 2012, Pages 673-682.

Griffiths, Mark D. and Davies, Mark N.O. (2003). *Breaking the stereotype: the case of online gaming*, Cyber Psychology & Behavior, Volume 6, Number 1, s. 81-91.

Howells, Karen. and Ertugan, Ahmet. (2017). *Applying fuzzy logic for sentiment analysis of social media network data in marketing*. Procedia Computer Science, v. 120, 664–670. Fedorov, Mykhailo. <https://twitter.com/fedorovmykhailo> Erişim Tarihi: 10,05,2022.

<https://42matters.com/> Erişim Tarihi: 14/05/2022.

<https://sozluk.gov.tr/> Erişim Tarihi: 14/05/2022.

<https://www.fbi.gov/wanted/cyber/apt-41-group> Erişim Tarihi: 14/05/2022.

<https://www.rbc.ru>. (2017). Rusya Güvenlik konseyi, çevrimiçi oyun kullanıcılarının kimliğini belirleme talimatı verdi, 27Kasım 2017.

https://www.rbc.ru/technology_and_media/27/11/2017/5a-1812759a7947098fd6b0b Erişim Tarihi: 14/05/2022.

<https://www.theguardian.com/uk-news/2021/oct/26/amazon-web-services-aws-contract-data-mi5-mi6-gchq?mid=1>).

<https://yokatlas.yok.gov.tr/lisans-bolum.php?b=18004> Erişim Tarihi: 14.05.2022.

<http://pravo.gov.ru/proxy/ips/?docbody=&nd=102404066> Erişim Tarihi: 14/05/2022.

<http://pravo.gov.ru> Erişim Tarihi: (2017). Terörizmle Mücadele Kanunu ve kamu güvenliğinin sağlanması için ek tedbirler alınması açısından “Terörizmle Mücadele Hakkında” Federal Kanununun ve Rusya Federasyonu’nun bazı yasal işlemlerinin değiştirilmesi hakkında kanun.

<https://www.usatoday.com/story/news/politics/2020/12/18/russian-cyber-attack-worst-may-yet-come-solarwinds-hacking/3956223001/>.

Huizinga, Johan. (2017). Homo Ludens. *Oyunun Toplumsal İşlevi Üzerine Bir Deneme*, Çev: Mehmet Ali Kılıçbay, Ayrıntı Yayınları: İstanbul.

Hünler, Arın. (2021). Küresel Pazarlara Giden Yol: Dijital Oyun Sektörü İzmir Kalkınma Ajansı, Şubat <https://startinizmir.izka.org.tr/kuresel-pazarlara-giden-yol-dijital-oyun-sektoru/>

Lordanou, Loanna. (2019). Venedik Gizli Servisi, Rönesans'ta bir istihbarat Teşkilatı, Çeviri: Fatih Yücel, Kronik Kitap: İstanbul.

Johnson Kevin, Snider. (2020). Mike, Pompeo says Russia 'prettyclearly behindcyberattack on US, but Trumpcasts doubtsanddownplaysthreat,, USA TODAY,20 Dec. 2020.

Kars, Gözde Bahar. (2010). *Şiddet içerikli bilgisayar oyunlarının çocuklarda saldırganlığa etkisi*, Disiplinler Arası Adli Tıp Anabilim Dalı Yüksek Lisans Tezi, Türkiye Cumhuriyeti Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, 2010: Ankara.

Kavsıracı, Ozan. (2020). *İstihbarat Süreci ve İnsan Kaynaklı İstihbaratın Analizi*. Uluslararası Toplum Araştırmaları Dergisi, 16 (27), 700-719.

Kavsıracı, Ozan. (2020). İstihbarat Süreci ve İnsan Kaynaklı İstihbaratın Analizi, Uluslararası Toplum Araştırmaları Dergisi, ISSN:2528-9527 E-ISSN: 2528-9535 Yıl Year: 10 Cilt Volume:16 Sayı Issue :27 Temmuz 2020.

Kenneth Araştırma, En İyi Ülke Verileriyle (2022-2031) Dijital Oyun Pazarı Büyüme Anketi: Büyüklük, Pay, Gelecekteki Büyüme, Kalkınma, Gelir, En Önemli Oyuncular Analizi ve Büyüme Faktörlerine Göre Sektöre Genel Bakış, 11 Mayıs 2022, <https://www.kennethresearch.com/sample-request-10085164>.

Kent, Steven L. (2000). İlk Çeyrek: Video Oyunlarının 25 Yıllık Tarihi, s. 83, BWD Press.

Kırcova, İbrahim. (2016) "*İnternette Pazarlama*", Beta Yayınları, İstanbul.

Koops, Bert Jaap. and Hoepman, Jaap-Henk. Leenes, Ronald. (2013). *Open-source intelligence and privacy by design*, Computer Law & Security Review, 29(6), 676–688.

Kurt, Ömür. (2016). Bilgisayar oyunlarının propaganda amaçlı kullanımı: Arap Baharı bağlamında “A forcemorepowerful” oyunu üzerine örnek bir araştırma, Bahçeşehir Üniversitesi/ Sosyal Bilimler Enstitüsü / Küresel Siyaset ve Uluslararası İlişkiler Bilim Dalı, Yüksek Lisans Tezi.

Leiner, Barry ve Cerf, Vinton. (1997). Wolff. *Brief History of the Internet* 1997, Internet Society, A Brief History of the Internet, internetsociety.org/wp-content/uploads/.

Liulevicius, Vejas Gabriel. (2011). *Espionage and Covert Operations: A Global History*, The Great Courses Corporate Headquarters 4840 Westfields Boulevard, Suite 500 Chantilly, The Teaching Company. Lowenthal, Mark and Robert Clark Ed. (2016). *The five disciplines of intelligence collection*, Thousand Oaks, CQ Press, an imprint of Sage Publications: California.

Machiavelli. (1994). *Prens*, Güvenç Nazım (Çev). İkinci baskı: Anahar Kitaplar Yayınevi.

Malone Tjomas ve Lepper Robert. (1987). Making learning fun: A taxonomy of intrinsic motivations for learning. In Snow R. E., Farr M. J. (Eds.), *Aptitude, learning, and instruction. Cognitive and affective process analyses* (sayı 3, s 223–253). Hillsdale, NJ: Lawrence Erlbaum.

Mazzetti, Mark. (2018). Lowenthal, *The Future of Intelligence*, Polity Press: Cambridge.

Mazzetti, Mark and Elliott, Justin. (2013). SpiesInfiltrate a Fantasy Realm of Online Games, Dec. 9, 2013, <https://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html>. Meta Reports Second Quarter 2022 Results, MENLO PARK, Calif., July 27, 2022. /PRNewswire/vMeta Platforms, Inc. (Nasdaq: META) June 30, 2022 Montesquieu, Kanunların Ruhü, De l’esprit

des lois, 1st edn 1748, 2 vols.1748. NGIA, National System for Geospatial Intelligence, Geospatial Intelligence (Geoint) basic Doctrine, National Geospatial –Intelligence Agency (NGIA) ,September 2006.

Norton-Taylor, Richard. (2012). “Former spy chief calls for laws on online snooping”, The Guardian, 24th of April, <https://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping> (Erişim:22/11/2022), National Security Agency, Games: A Look At Emerging Trends, Uses, Threats And Opportunities In Influence Activities, 2007 <https://grid.glendon.yorku.ca/exhibits/show/security-classification/item/464>.

Omand, Sir David. and Bartlet, Jamie. and Miller, Carl. (2012). “Introducing social media Intelligence (SOCMINT)” in Intelligence and National Security, Vol.27. No. 6, December.

Oosthoek, Kris and Doerr, Christian. (2021). *Cyber Threat Intelligence: A Product Without a Process?* International Journal of Intelligence and CounterIntelligence, 34:2, 300-315.

Özçam, Tansu. (2019). Çevrimiçi şiddet ve dijital oyun pratikleri bağlamında counterstrike global offensive örneğinin analizi, Kocaeli Üniversitesi / Sosyal Bilimler Enstitüsü Gazetecilik Yüksek Lisans Tezi, 2019 s105-110.

Özdağ, Ümit. (2018). *İstihbarat Teorisi*, Kripto Yayınevi, 13. Baskı: Ankara.

Özkaya, Ömer. (2006). *CIA Belgeleriyle Zihin Kontrol Operasyonları, Pegasus Yayınları*: İstanbul.

Palmer, Danny. (2019). Chinese cyberspies are stealing Money from video game firms on the side, August 7, 2019 <https://www.zdnet.com/article/chinese-cyber-spies-are-stealing-money-from-video-game-firms-on-the-side/>.

Partleton, Kayleigh. (2021). Ten Square Games saw \$153 million in revenue last year, <https://www.pocketgamer.biz/news/76142/ten-square>

re-games-saw-153-million-in-revenue-last-year/Renatus, Flavius Vegetius. (2019). *Roma Savaş Sanatı*, Çeviren, Samet Özgüler, Kutsi Aybars Çetinalp, Kronik Kitap, 1.ci baskı: İstanbul.

Rovner, Joshua. Intelligence in the Twitter Age, *International Journal of Intelligence and Counter Intelligence*, 26:2, 260-271, 2013.

Scott, Len. And Jackson Peter. (2004). "Journeys in Shadows", *Understanding Intelligence in the Twenty First Century: Journeys in Shadows*, Len Scott ve Peter Jackson (Eds.), New York: Routledge.

Snider, Mike. and Jessica, Guynn. (2020). How Russian spy games moved online: Massive breach shows how espionage is carried out in the 21st century, 19 December 2020, <https://finance.yahoo.com/news/russian-spy-games-moved-online-014024848.html>.

Stilwellblake, Savaş. Alanında Birlikleri Eğitmek İçin Kullanılan 6 Askeri Video Oyunu, 13 Mayıs 2016. www.military.com/underthedar/2016/05/6-military-video-games-used-to-train-troops-on-the-battlefield.

Soyak, Ahmet Selman. (2022). Büyük Şirketlerin Gözü Dijital Oyunlarda, Mart 2022, <https://www.guvenlioyuna.org.tr/haber-detay/buyuk-sirketlerin-gozu-dijital-oyunlarda>.

Şimşeker, Somer Alp. (2022). *Osmanlıda İstihbarat*, ikinci Şube Tarihi, Kronik Kitap.

Tekin, Muhammet. (2016). *New Perspectives on Intelligence Collection And Processing*, Yüksek Lisans Tezi, Naval Postgraduate School Monterey: California.

Telci, Aygün Şen. (2013). Siber Uzamda Sosyal ve Kültürel Kodların Oyun Aracılığıyla İnşası: "İstanbul Kıyamet Vakti". XV. Akademik Bilişim Konferansı Bildirileri (23-25 Ocak 2013). https://ab.org.tr/ab13/kitap/telci_AB13.pdf: 783- 782.

Tirnovalı, Sercan. (2019). *Dijital Oyunlar Üzerinden Karşı İstihbarat Toplama ve Bilgi Edinme: Assassin's Creed Örneği*, Yüksek Lisans Tezi İstanbul Aydın Üniversitesi.

Tirnovalı, Sercan. (2019). Dijital oyunlar üzerinden karşı istihbarat toplama ve bilgi edinme: Assassin'screed örneği, İstanbul Aydın Üniversitesi / Sosyal Bilimler Enstitüsü / Siyaset Bilimi ve Uluslararası İlişkiler Ana Bilim Dalı / İstihbarat Bilim Dalı Yüksek Lisans Tezi.

Traynor, Lan. (2007). Russia accused of unleashing cyber war to disable Estonia 17 May 2007, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

Ünal Seyfettin ve Gök Ömer. (2022). *Uluslararası Sistemde Yeni Ekonomik Alanlar: Dijital Oyun Piyasaları, Gelişimi ve Türkiye Üzerine Etkileri.*”, Uluslararası Sistemin Yarattığı Sorunlar ve Çözüm Yolları”, 30-31 MAYIS 2022/ANKARA) Kongre Bildiri Tam Metin Kitabı, Stratejik Düşünce Enstitüsü Yayınları,2022. www.mit.gov.tr/text_site/isth-olusum.html Erişim Tarihi: 14/05/2022.

Yarar, Hamza. (2019). *Simülasyon ve dijital kitle süsü: Çok oyunculu çevrimiçi mobil oyunlar üzerine bir analiz*, Fırat Üniversitesi, Sosyal Bilimler Enstitüsü, İletişim Bilimleri Ana Bilim Dalı, Yüksek Lisans Tezi, 2019s.110-125.

Yığıtoğlu, Vedat. (2018). *Oyun değer-dijital oyunlar ve kullanıcılar üzerine bir inceleme: To the Moon Örneği*, Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü, Halkla İlişkiler ve Tanıtım Ana Bilim Dalı, Doktora Tezi, s.195-215. Yung Chang Ku ve Ying-Chieh: Chen,Kuo-Ching Wu and Chaochang Chiu. (2007). An empirical analysis of online gaming crime characteristics from 2002 to 2004, PAISI'07: Proceedings of the 2007 Pacific Asia conference on Intelligence and security informatics April 2007s 34-45.

Ziółkowska, Agata. (2018). *Open source intelligence (OSINT) as an element of military recon*, War Studies University, Faculty of National Security, Security and Defence Quarterly 2018;19(2):65-77 M.E.B 2022 2021 YLSY –https://yyegm.meb.gov.tr/meb_iys_dosyalar/2021_11/05093016_2021_YLSY_Secme_Min_Max_Duzenli.pdf

Extended Summary

Digital games have started to show their presence in every aspect of our lives. Today, individuals of all ages, from the age of 7 to the age of 70, now spend an important part of their time on these digital platforms, sometimes for spending time, sometimes for entertainment, and sometimes for financial gain. These delays can lead to undesirable results. It is possible to establish friendships with people in the virtual world in front of us or next to us, without knowing their real-world identities, and share the most private information willingly or unwillingly.

The relationship between the digital world and intelligence begins to be interrelated at the point of revealing the purposes behind secret friendships. The information received during the game with sociological methods, both live in the game and before or after the game, through the connection methods, shared spatial information, are serious data sharing from the individual to the country. In these platforms, it appears in the form of information sharing in a deep and wide range, ranging from the aims of obtaining financial gain from the organizations and or the organizational staff, from their goals to the goals of obtaining moral gain. The relationship between digital game markets, which is a new subject in our country, and intelligence, which has only been found in a study so far, has been tried to be examined. The effect of intelligence, which is the most private point of the states, on the digital world and games, the struggles of China, Russia and the USA in the digital world are explained with examples, with the fact that the digital world is also used in this regard from the disclosures of J. The fact that the companies in the digital game market are supported by the state and how much effect they have in the market economically have been revealed by the data. In our country, the importance of investing in the necessary human resources and the necessity of raising awareness in terms of security are emphasized.

In the first part of our article, the introduction to the science of intelligence, the importance of intelligence in the historical process, the purposes of use, its types according to the fields, the intelligence activities

of the countries and administrators, which identity and how they use other elements are discussed. In our country, the types of intelligence in the academic field, political, military, economic, social, geographical, biographical, transportation and communication, scientific and technical intelligence, social media and the development of smart device systems and devices, and the diversity of cyber intelligence and information wars have been discussed. The digital world and digital intelligence concepts, the development of information and technology, with the effect of globalization, in our age where we can not keep up with the speed of information and technology, with the introduction of the digital world into our mobile phones, the desire of intelligence organizations to follow every field in order to prevent disinformation activities, where false and true, true and false information spreads easily. He introduced the concept of intelligence (SOCMINT). Social media platforms in the world were examined and statistics such as daily usage times and number of members were given. It is considered that there are serious indications that social media intelligence (SOCMINT) is used by institutions and organizations, as well as malicious people and organizations, and that they cause security vulnerabilities in terms of the scope in which this issue is discussed in the world.

In the second part of our article, the concepts of game and digital game are discussed. It has been revealed that digital games are presented together with real life and virtual reality, appeal to all age groups where they are a part of social life, and give the same pleasure as the reality with the visuals, sounds, movements they contain according to their genres, thus creating a commitment. By nature, people adapt to the environment in which they are constantly interacting, adapt to the digital environment reflected in digital games, enter and accept the rapid learning process, and in this context, the industry is constantly renewing and developing, in this context, it has gained an important place in the field of international trade, and energy and energy, which are the building blocks of trade. It has been tried to reveal that the change in smart phone and tablet technologies, with the effect of the Covid-19 epidemic, which has entered a fast-growing

phase by leaving the automotive sectors behind, caused an increase in digital game playing times thanks to computer and game consoles. The data on the reports and statistics published in Türkiye and other countries on the digital game market were examined, and in this context, it was tried to be revealed with the data that digital games could reach a financial size in the future. The relationship between intelligence and the game, which is the subject of the first and second parts of our article, has been revealed by examining the master's and doctoral studies registered in the YÖK Thesis system and by examining the studied and unstudied subjects.

In the third part of our article, the relationship between the ways that digital games affect the individual and intelligence is discussed. Individuals digital.