**AKILLI KENTLER VE DİJİTAL (SİBER) GÜVENLİK\***

***Hayriye ŞENGÜN[[1]](#footnote-1)\*\****

***Abdülsamet KOÇHAN[[2]](#footnote-2)\*\*\****

***Seçil Gül MEYDAN YILDIZ[[3]](#footnote-3)\*\*\*\****

**Öz**

Kentler, tarihin ilk çağlarından bu yana, teknolojideki gelişmelerin etkisiyle sürekli değişim ve dönüşüm göstermektedir. Endüstrileşme ile birlikte kentler, insanların yoğun yaşadığı, gelişen ve değişen gereksinimlerin karşılandığı mekânlar olmuştur. Teknolojik gelişmeler yapı tarzlarının yanı sıra kentlerin biçimlenişinde de farklılıklara yol açmıştır. Ekonomik ve teknolojik gelişmelerin etkisiyle giderek nüfusları artan kentlerin, yaşayanların huzur ve güvenliğini sağlamak için yeni yönetim modelleri denemek durumunda kaldıkları görülmektedir.

Kentlerin giderek kontrol edilemez büyüklüklere ulaşması, bilişim teknolojisinin kendisine yeni bir uygulama alanı bulmasıyla birlikte, kent yönetimleri, kentsel hizmetleri akıllı uygulamalarla donatmaya başlamıştır. Akıllı uygulamaların kentlerdeki etkinliği arttıkça bu uygulamalara yönelik siber saldırılar ve tehditler de artacaktır. Uluslararası çabaların rekabeti tetiklemesi, kötü niyetli güçlerin kentsel güvenliği tehdit edecek eylemlere kalkışması, sık karşılaşılan bir durum olarak kendini göstermektedir. Dünyadaki uluslararası ilişkiler giderek barışçıl niteliğini kaybederken, bu gibi saldırıların olmayacağı düşünülemez. Siber saldırılarla ilgili olarak gerekli önlemlerin alınmaması bu teknolojiyi üretmeyen ülkelerde önemli sorunlara yol açabilecektir.

Bu çalışmada, sayıları giderek artan akıllı kentlerin siber tehdit karşısında ne denli güvenli olduğu ve yaşanabilecek siber sorunların niteliği araştırılmaktadır. Çalışma, Türkiye’deki akıllı kent uygulamaları ile sınırlıdır. Literatür tarama yöntemiyle konuya ilişkin verilere ulaşılarak, gelecekte yoğun kullanılacağı tahmin edilen akıllı kent uygulamalarının karşılaşacakları olası siber tehlikelerin neler olabileceği değerlendirmektedir.

**Anahtar Kelimeler:** Akıllı Kent, Siber Güvenlik, Siber Saldırı, Akıllı Kent Bileşenleri, Hacker

**SMART CITIES AND DIGITAL (CIBER) SECURITY**

**Abstract**

Cities have been constantly changing since the first ages of history with the effect of technological developments. With industrialization cities have become places developing and changing requirements have been met and where people live intensively. Technological developments have led to differences in the shape of the cities as well as the building styles. With the impact of economic and technological developments, they had to try new management models to ensure the peace and security of the inhabitants of the growing population.

With the cities becoming increasingly uncontrollable, with the new technology of information technology, urban governments have begun to equip urban services with intelligent applications. As the effectiveness of smart applications in cities increases, cyber attack sand threats to wards these applications will also increase. Today, one cannot deny the effect of the intense efforts of international companies that have a say in smart city applications in order to build smart applications one after the other. These international efforts are triggered by competition, and some anti-government forces are taking advantage of the possibilities of information technology to act as a threat to urban security. As the effectiveness of smart applications in cities increases, cyber attack sand threats to wards these applications will also increase. The fact that international efforts triggered competition and malicious forces attempted to threaten urban security is a common case. While international relations in the world are gradually losing their peaceful character, it is unthinkable that such attacks will not occur. Taking necessary measures in relation to cyber attacks may also cause significant problems in countries that do not produce this technology.

In his study, the safety of the number of smart cities in the face of cyber threats and the nature of the cyber problems that can be experienced are investigated. The study is limited by the smart city applications in Turkey. With the literature scanning method, the data on the subject is reached and evaluates the possible cyber hazards that the smart city applications, which are predicted to be used intensively in the future, will face.

**Keywords:** Smart City, Cyber Security, Cyber Attack, Smart City Components, Hacker.

**GİRİŞ**

Tarihin ilk çağlarından beri kentlerin ortaya çıkışı ile birlikte, kentte toplanan artı ürünün korunmasının yanı sıra yaşayanların güvenliği de bir sorun olarak algılanmıştır. Tarihsel gelişim süreci içerisinde kentler hem bilimsel gelişmelerin üretildiği mekân hem de bu bilimsel gelişmelerin ürünlerinin kullanım alanı olmuşlardır. Günümüzde bilimsel ve teknolojik gelişmelerin düzeyi, yeni ve farklı bir yaşam biçimine kaynaklık etmektedir. Kentlerdeki birçok hizmet, bilgi teknolojisinin kullanım alanı haline gelmiştir. Kentsel mekânda bu yeni teknoloji ürünlerinin kullanılmasıyla birlikte kentlerde yaşayanların yaşamını kolaylaştıran ve hizmet üretiminde zaman tasarrufu yaratan sonuçlar ortaya çıkmaktadır. Günümüz dünyasında küreselleşmenin de etkisiyle çok hızlı gelişmeler yaşanmakta, ülkeler ve kentler arasında ekonomik, sosyal, kültürel ve yönetsel etkileşim alanları da her geçen gün artmaktadır. Kentlerin yarışmacı bir anlayışın etkinlik alanı haline gelmelerinde, günümüzdeki bilimsel gelişmelerin bunu kaçınılmaz kılmasının rolü çok fazladır.

Türkiye’de olduğu gibi dünyada da kentlerde yaşayan insan sayısı her geçen gün artmaktadır. Kentler, bu kalabalık nüfusun kentsel hizmetlere erişimini kolaylaştırmak, kentsel hizmetlerin sunulmasını etkin ve verimli hale getirmek için yeni ve modern teknolojilerden olabildiğince yararlanmanın çabası içerisindedir. Kentsel nüfustaki hızlı ve düzensiz artış, kent ve çevre değerleri üzerindeki olumsuz etkinin giderilmesine olanak sağlayacak yeni yönetim bileşenlerini gerektirmektedir. Bilişim teknolojisinin olanaklarından yararlanarak, kentsel hizmetlerin hızlı, etkin ve verimli olmasını sağlayacak bu yeni bileşenler insan etkisinin en az düzeyde olduğu bilişim teknolojisi ürünü yazılım programları olarak karşımıza çıkmaktadır. Bilişim teknolojisinin yaşamın her alanında etkinliğinin artması insanlar, ülkeler ve kentler arasındaki rekabeti de artırmaktadır. Bu rekabetin yapıcı etkilerinin yanında, ülkelerin ve insanların başkaları üzerinde egemenlik kurma isteği gibi yıkıcı riskleri de bulunmaktadır.

Bilgi teknolojilerinde yaşanan hızlı gelişmeler ve küreselleşme sürecinin etkisiyle kentlilerin değer sistemleri giderek farklılaşmakta ve insanlar kent yönetimlerinden daha farklı beklentiler içine girmektedir. Dünyadaki bu değişimler kentsel hizmetlerin sürekli yenilenmesini ve yeni gelişmelere ayak uydurulmasını zorunlu hale getirmektedir. Günümüz dünyasında bilişim teknolojilerinden bağımsız sosyal yaşam söz konusu olmadığı gibi ekonomik yaşamın da bu gelişmelerden bağımsız olması düşünülemez. Küreselleşme ile sermayenin serbest dolaşımının yanı sıra bilginin de serbest dolaşımı ve erişilebilirliği artmıştır. Küreselleşmenin dayattığı koşullarda yeni pazar alanlarından birisi de bilişim sektörü ürünlerinin kentlere yönelttiği akıllı uygulamalardır. Bilişim alanında öncü şirketlerin kentsel hizmetlere ilişkin geliştirdikleri yazılımlar veya yeni kent tasarımlarında her türlü ayrıntıyı bilişim yazılımlarıyla kurgulamaları, kentleri bu uygulamaları kullanma konusunda da yarışır hale getirmiştir.

Dünyadaki ekonomik ve siyasi ortamdaki rekabet unsurları her zaman dengeli ve barışçıl bir ilişki kurmak amacıyla yürütülmemektedir. Günümüzde egemenlik sınırları coğrafi sınırlarla değil, ekonomik etkinlik alanlarıyla da tartışılmaktadır. Ulusal sınırları aşan bu egemenlik tartışmalarında siber güvenlik tartışmaları en önemli noktaya oturmaktadır. Bilişim teknolojilerinin uygulamalarının temelinde bilişim teknolojisinin çıktılarının olması, bu teknolojileri geliştiren veya bu gelişme eğilimlerine müdahale edebilecek birikimi olanların saldırı ve korunma davranışlarının mücadele alanı olmaktadır. Dijital güvenlik veya siber güvenlik olarak literatüre geçen bu korunma süreçlerinin kontrolü de bilişim teknolojisine ve bu teknolojiyi kontrol gücüne sahip olmayı gerektirmektedir.

Bu çalışmada kentlerde giderek artan akıllı uygulamaların güvenli kullanımına yönelik tehditlerin neler olabileceği ve bu konuda ne gibi gelişmeler olduğunun tartışılması amaçlanmaktadır. Tartışmanın kapsamı kentsel altyapı ve yönetim süreçlerinde kullanılan bilişim teknolojisinin uygulamalarıyla sınırlıdır. Çalışmada literatür tarama yönteminden yararlanılmıştır. Bu çalışmanın çıktısını, akıllı kent uygulamalarının kurulması ve işletilmesi kadar, dijital güvenlik konularının tartışılmasının sağlanmasının önemi oluşturmaktadır.

**I. KAVRAMSAL ÇERÇEVE**

**1.1. Akıllı Kent**

Yerleşik düzene geçilmesiyle başlayan kentsel sistemler, aynı zamanda uygarlığın yansımaları olarak da önemli işlevler yürütmüşlerdir. Ticaretin, sanayinin, kültürün ve eğitimin yeşerdiği yerler olarak kentler bugün de bilimin, sanatın ve diğer gelişmelerin ortaya çıkmasına kaynaklık etmektedir. Genel anlamda kenti tanımlamak için geçmiş yüzyıllarda kale ve sur olarak referans alınan değerler bugün ekonomi biliminin aktörleri olan istihdam, ekonomik işlevler ve işbölümü gibi etkinlik alanları ile tanımlanmaktadır (Yılmaz ve Çiftçi, 2011: 255). Bugünkü işlevleri ile kent; tarım dışı üretimin yapıldığı, üretim yapılan alanlardaki sürecin denetlendiği, dağıtımın eşgüdümlü bir şekilde gerçekleştirildiği, kırdan farklı ve yoğun üretim tarzının aynı zamanda farklı bir yaşam tarzını da beraberinde örgütlediği, farklı nüfus görünümlerini de içinde barındıran bir yerleşim birimi ve yaşam alanı olarak tanımlanabilir. Günümüz dünyasında kimilerine göre kent; sürekli bir devinim ve yoğun bir iş enerjisinin yanı sıra olağanüstü yeniliklerin gerçekleştiği yerdir. Kimilerine göre ise kent; tüketimin yanı sıra yeni şeyler bulmak için tahrik edici ve pahalı olanakların olduğu bir oyun bahçesi olarak görünür (Herzberg, 2018: 19).

Teknoloji yönelimli kentsel tasarımlar 2000’li yılların başından itibaren bilgi toplumu kavramsallaştırması içerisinde kentlerde mekânı dönüştürmeye başlamıştır. Nitelikli işgücünü kendilerine çekmeyi de öncelikli hedef edinen ve bu doğrultuda kentsel stratejiler geliştiren, Dubai, Singapur, Barselona, Melbourne, Boston, Manchester gibi dünya kentleri önemli adımlar atmışlardır. Yeni kentsel stratejilerde ağırlıklı yönelim teknolojik bakış açısının kentsel ve toplumsal yaşama uyarlanmasıdır.

Kentlerin her geçen gün artan nüfusu ve yetersiz altyapısı gelişen teknolojilerle desteklenerek daha yaşanabilir mekânlar üretilmesinde kullanılmaktadır. Bu yeni kentsel oluşumun temel aktörlerinin bilişim teknolojisinin akıllı uygulamaları olması, bu teknolojiyi kullanan kentlerin de akıllı kent tanımlanması ile anlatılmasına kaynaklık etmektedir. Bir kenti akıllı yapan şey, kentsel temel hizmetleri halka daha etkin sunabilmek amacıyla akıllı bilişim sistemlerinin kullanmasıdır. Akıllı kent kavramıyla tanımlanan bu yeni kentsel yaklaşım giderek yaygınlaşmaktadır. Zeki Kent, Bilgi Kenti, Sürdürülebilir Kent, Yetenekli Kent, Kablolu Kent, Dijital Kent, Eko- Kent (Uçar vd., 2017: 1787) gibi kavramlarla da anlatılmaya çalışılan kavramın net bir tanımı henüz yapılmamış olsa da “akıllı kent”, akıllı kent altyapısı ve hizmetlerinin bir koleksiyonu olarak nitelendirilmektedir. Akıllı kent, kentlerdeki kritik altyapı bileşenlerinin ve kentsel yönetimin, kamu güvenliği, eğitim, ulaşım, sağlık, gayrimenkul gibi kamu hizmetlerinin akıllı bilgi işlem teknolojileri kullanılarak daha akıllı ve daha verimli hale getirildiği kentlerdir (Washburn ve Sindhu, 2010). Velibeyoğlu (2016) ise, akıllı kentleri, fiziksel dünyanın içine sanal uygulamaları entegre ederek etkileşimli alanlar yaratan bilgi ve iletişim teknolojilerine sahip akıllı ortamlar olarak tanımlanmaktadır. Diğer bir deyişle akıllı kentler; kentlerde bilgi iletişim teknolojilerinin ve sensörlerinin gündelik yaşamda seyahat ederken, çalışma yaparken kullanılan fiziksel nesnelerin içine gömülmesi ile görünmez oldukları fiziki ortamlar haline gelmesi olarak adlandırılmaktadır (Stratigea, 2012). Akıllı kentler aynı zamanda insan aklının ürünü olan bilgi ve iletişim teknolojilerini kentin yaşanabilirliğini, çalışılabilirliğini ve sürdürülebilirliğini sağlamak için kullanabilen kentlerdir (Kamu Teknoloji Platformu, 2016: 10-13). Kentlerde bu dijital teknoloji ürünlerinin kullanılmasında temel amaç, kentle ilgili riskleri ölçmek ve belirsizlikleri yönetmektir. Özellikle kamu hizmetleri, altyapı, enerji, ulaşım, inşaat, sağlık, çevre ve tarım alanlarında kullanılan birçok farklı akıllı kent teknolojisi bu alanlarda etkinliği ve verimliliği artırmaktadır.

Akıllı kent hem düz hem de mecazi (değişmeceli) bir tanım niteliği taşımaktadır. Bazen bir kentin bir parçası, ancak istisnasız olarak kent sakinlerinin kentin geleceğinin en önemli bir parçası olarak dijital teknolojiye kucak açtığı bir yerdir. Bu kentler birçok biçimde ve farklı derecelerde akıllı olarak kurulacak olsalar da, en temel ilke, kentsel hizmetlerin tek bir platformda toplanmasıdır. Tarihsel olarak ayrı ve verimsiz olan bu hizmetler dijitalleşme yoluyla birbirine bağlanabilmekte ve iyileştirilebilmektedir (Herzberg, 2018: 21).

Akıllı kentlerde kentsel teknolojiler temel altyapıyı oluşturmakta, kentin gerçek zamanlı analizinde ve değerlendirilmesinde Coğrafi Bilgi Sistemleri (CBS) veri tabanlarından, sanal gerçeklik ve simülasyon (benzetim) teknolojilerinden yararlanılmaktadır. Mobil-kablosuz iletişim, internet erişimi, kablolu, dijital yayıncılık, dijital kent ekranları gibi bilgi ve verilerin gerçek zamanlı iletimi ve yayılımını düzenleyen teknolojiler kullanılarak kentsel geleneksel hizmetlerin yerini alması, akıllı kentlerin temel prensibini oluşturmaktadır. Kentsel mekânların yeni bileşenleri olarak; “esneklik”, “mobilite”, “bağlanabilirlik”, “ağ örüntüsü” gibi kavramlar öne çıkmaktadır.

**1.2. Siber Güvenlik ve İlgili Kavramlar**

*Siber* kelimesi, bilişim sistemleri altında çalışan soyut ve geniş bir alt yapıyı ifade etmektedir. Buna kısaca “siber uzay” (âlem) da denilmektedir. Siber âlemin ana aktörü olarak internet; küresel internet protokol sistemini (TCP/IP) destekleyen aygıtları ve ağları birbirlerine bağlayan, insanların ve bağlı aygıtların birbirleri arasındaki etkileşimi ve iletişimi sağlayan ağ olarak “nesnelerin interneti” konseptinin temel altyapısını oluşturmaktadır (<https://donencebilisim.com>). Sayısal bilgileri depolayabilen veya işleyebilen hemen hemen her bilgisayar aygıtı siber alanın bir parçası olarak düşünülebilir (Goychayev vd., 2017).

*Siber uzay* terimi ilk kez William Gibson’ın “Neuromancer” adlı romanında kullanılmış ve daha sonra yaygınlık kazanmıştır (Kut, 2013: 2). İnternetin ilk çıktığı zamandan bu zamana kadar her geçen gün daha fazla insanın yaşamını meşgul ettiği ve yaşamın her alanına dâhil olduğu, aynı zamanda insanların kendi kimlikleri yanında sosyal hayatlarında da kimlik sahibi olmasına olanak sağladığı görülmektedir.

Kişinin veya toplumun hassas ve değerli olarak gördüğü varlıklara yönelik herhangi bir zarara, hasara ve kötülüğe karşı korunma veya karşı koyma derecesi anlamında kullanılan kavram olarak *güvenlik,* Türk Dil Kurumu Türkçe Sözlüğünde; “Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet” ([www.tdk.gov.tr](http://www.tdk.gov.tr), 2019) olarak açıklanmaktadır. *Siber güvenlik* ise, kavramsal olarak bilişim ve yazılım tabanlı sistemleri, ağları ve programları dijital saldırılara karşı koruma uygulamasıdır. Bu siber saldırılar genellikle hassas bilgilere erişmeyi, değiştirmeyi veya imha etmeyi amaçlamakta; kullanıcıların hesaplarından para çekmek veya normal iş süreçlerini kesintiye uğratmak olarak sıkça görülmektedir. Etkili siber güvenlik önlemlerinin uygulanması her geçen gün daha fazla gündem oluşturmakta, ancak siber alanda güvenliği sağlamak da o denli zor olmaktadır. Bu tehditlerin ve saldırıların fazla olmasında, insanlardan daha fazla dijital teknoloji için kullanılan cihazların olması ve saldırganların giderek daha yenilikçi gelişmeleri biliyor hale gelmesi önemli bir etkendir. (<https://emoji.com.tr>, 2019)**.**

Başarılı bir siber güvenlik yaklaşımı, bilgisayarlarda, ağlarda, programlarda veya güvende tutmak istediği verilerde yayılan birden fazla koruma katmanına sahiptir ([www.cisco.com](http://www.cisco.com), 2019). Bir örgütte insanlar, süreçler ve teknoloji, siber saldırılara karşı etkili bir savunma oluşturmak için birbirlerini tamamlamalıdır ([www.cisco.com](http://www.cisco.com), 2019). Günümüzün networklerle birbirine bağlı dünyasında, herkes gelişmiş siber savunma programlarından yararlanmaktadır. Bireysel düzeyde, bir siber güvenlik saldırısı kimlik hırsızlığından, zorla girme denemelerine, aile fotoğrafları gibi önemli verilerin kaybolmasına kadar her şeyle sonuçlanabilmektedir. Herkes enerji santralleri, hastaneler ve finansal hizmet şirketleri gibi kritik altyapıya güvenmektedir. Bunları ve diğer kuruluşları güvence altına almak ve toplumsal yaşamın devamlılığını sağlamak için çalışır durumda tutmak esastır ([www.cisco.com](http://www.cisco.com)). Bütün ülkeler ortaya çıkan tehditleri ve siber saldırı stratejilerini araştıran siber tehdit araştırmacılarının çalışmalarından da faydalanmaktadır. Buna örnek olarak Talos’taki 250 tehdit araştırmacısı ekibinin çalışmaları gösterilebilir. Bu ekibin çalışmaları ile yeni güvenlik açıkları ortaya konulmakta, halk siber güvenliğin önemi konusunda eğitilmekte ve açık kaynak araçları güçlendirilmektedir. Bütün çabaların temelinde, interneti herkes için daha güvenli kılma düşüncesi yatmaktadır ([www.cisco.com](http://www.cisco.com), 2019).

Siber güvenlik kavramı, internetin gündelik yaşama uyarlanması ve bu internet içerisindeki güvenlik kaygılarının ortaya çıkmasıyla yakından ilgilidir. Kavram, tüm dünyada sık sık gündeme gelmekte ve bu konuyla ilgili devletler tarafından eğitimler, etkinlikler, çalışmalar yapılmaktadır. Artık sadece bireylerin değil, devletlerin, kamu kurumlarının, sosyal platformların, KOBİ’lerin, özel şirketlerin sunmuş oldukları tüm hizmet ve ürünlerin iletişimleri de sanal ortamlar üzerinden sağlanmaktadır. Bu durumda tüm bilgi ve veri kaynakları sanal sistemlerde birikmektedir. Bu durum hizmetler ve kaynaklar açısından büyük bir tehlike oluşturmaktadır.

Siber güvenliğin kapsamı, internet kullanımının evreni olarak tanımlanabilecek siber uzayın tamamı olarak kabul edilmektedir. Siber güvenliğe, sadece internetteki sanal ve fiziksel sistemlerin güvenliğini kapsayan yapay zeka ve makine öğrenimi, aynı zamanda “kriptografi” gibi birçok bilim dalından yararlanan teknik bir alan olarak yaklaşmak doğru olmayacaktır. Siber güvenlik, kendisi de alt dallara sahip olan, bilgisayar biliminin bir alt dalıdır. Siber güvenlik konusunda öncelikli olarak devletlerin yasal düzenleme yapma, politikalar belirleme yükümlülükleri vardır. Sadece bununla kalmayıp kamu ve özel sektörün ya da uluslararası diğer örgütsel yapıların da bu alanın düzenlenmesine yönelik stratejik planlamaları bulunmaktadır. Buradan anlaşıldığı üzere, siber güvenliğin hem hukuksal hem siyasal hem de yönetimsel boyutu bulunmaktadır (http://afyonluoglu.org, 2019).

Siber güvenlik akıllı kent ilişkisine bakıldığında, akıllı kentsel çözümleri ve bunları kullanacak kentlileriyle akıllı kentler de siber uzayın bir parçasıdır. Geniş bir yayılma alanına ve yükselen potansiyele sahip olan akıllı kentlerin, siber uzayın karanlık tarafının da ilgi ve odak noktası olması beklenmektedir. Bu nedenle her türden aygıtın ve insanların büyük çoğunluğunun internete bağlı olduğu akıllı kentlerde gerçekleşecek bir siber saldırının etkisinin büyük olacağı açıktır (Çelik, 2018:112-115). Kentlere yönelik kötü niyetle gerçekleştirilecek ve etkili olacak bir siber saldırı sonucunda, kentsel yaşam süreçleri olumsuz etkilenecek, kentin kaynakları boşa harcanacak ve altyapı sistemleri zarar görecektir. Bununla da kalmayacak, gizli verilerin kötü niyetli kişilerin eline geçmesiyle kentsel işlemler yavaşlayacak hatta durma noktasına gelebilecektir. Gerçekte daha yaşanabilir ve sürdürülebilir yaşam sunmayı amaçlayan akıllı kentler, bir siber saldırı ile vadettiklerini sunamayacak ve akıllı kent olmaktan uzaklaşacaklardır. Bu ve benzeri olumsuzluklarla karşılaşılmaması için akıllı kentlerde de siber güvenliğin öneminin kavranması ve kentte yaşayan akıllı sistemlerin kullanıcısı durumundaki her bir bireyin siber güvenlik ile ilgili farkındalığının oluşturulması gereklidir (http://afyonluoglu.org, 2019)**.**

**II. AKILLI KENTLER VE SİBER GÜVENLİK**

Bir kentin akıllı olarak nitelendirilebilmesi için, dijital teknolojilerin etkin kullanımı ile akıllı ekonomi, akıllı ulaşım, akıllı yönetişim, akıllı yaşam, akıllı vatandaş, akıllı çevre bileşenlerinin kentte dönüşüm sürecini gerçekleştirdiği bir yapıdan söz etmek gerekmektedir (Uçar, 2017: 1789- 1793) Avrupa, Amerika, Çin gibi gelişmiş teknolojilere sahip ülkelerde kentin stratejik planlarına entegre edilen akıllı uygulamalar, Türkiye’de de İstanbul, İzmir, Ankara, Bursa, Kayseri, Yalova vb. pek çok kentte parçacıl uygulamalar olarak hayata geçirilmiştir. Türkiye’de 2025 yılına kadar, 26 kentin “Akıllı Kent” niteliğine kavuşacağı açıklanmaktadır ([www.emlaksayfasi.com.tr](http://www.emlaksayfasi.com.tr), 2019). Gün geçtikçe akıllı uygulamaları hayata geçiren kentlerin sayısı ve uygulamaların çeşitliliği artmaktadır. Ancak burada temel sorun akıllı kentlerin; akıllı teknoloji, akıllı ulaşım, akıllı bina, akıllı enerji, akıllı altyapı, akıllı sağlık hizmetleri ve bu akıllı uygulamaları kullanma becerisine sahip akıllı kentlilere ne denli sahip olduğu gerçekliğidir.

Akıllı kent uygulamaları kentsel yaşama ilişkin temel verilerin, çeşitli yazılımlar ile yürütülmesi olduğuna göre, bu yazılımların sürdürülebilirliğinin sağlanması da aynı zamanda bir güvenlik sorununu beraberinde getirmektedir. Örneğin, akıllı ulaşım sistemine yapılacak bir dijital müdahale bütün trafik düzeninin bozulmasına yol açabilir. Aynı şekilde akıllı enerji uygulamasının bir müdahale ile karşılaşması bütün sistemin kullanımını olumsuz etkileyebilecektir.

Günümüz teknoloji dünyasında güçler arası çatışmalarda eksen kaymaları yaşanmaktadır. Amerikan seçimlerine Rusya’nın müdahale ettiği iddiası, başka ülkelerdeki dijital sistemlere çeşitli ülkelerin hackerlarının saldırı tartışmaları ([www.haberturk.com](http://www.haberturk.com), 2019), akıllı kent uygulamalarının da tehdit altında olduğunu ve siber güvenliğin ne denli önemli olduğunu ortaya koyan ciddi bir olgudur. Siber güvenlik bağlamında dikkat edilmesi gereken konular aşağıdaki gibi sınıflandırılabilir.

**2.1. Kişisel Verinin Korunması**

Kişisel veri kavramı, 24.03.2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda (KVKK) “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” şeklinde tanımlanmaktadır. (KVKK, 2016). Bu bilgiler içerisinde bireyi tanımaya yarayan özgün bilgilerin (adı, soyadı, anne adı, baba adı, doğum tarihi, doğum yeri gibi) yanı sıra, diğer (fotoğrafı, ev ve e-posta adresi, banka bilgileri, tıbbi bilgileri, sosyal medyadaki paylaşımları veya bilgisayarının IP adresi gibi) fiziksel, fizyolojik, ekonomik, kültürel, sosyal veya psikolojik pek çok bilgiyi de içermektedir (<http://afyonluoglu.org>, 2019). Kanun’la kişisel veri olarak tanımlanan bilgilerin, ilgili kişilerin izni olmadan kullanılması yasaklanmıştır. Kanunu ihlal edenlere ve veri ihlali yapanlara yönelik ciddi cezalar getirilmektedir.

Kentlerin, hizmetleri daha hızlı, ucuz ve kentlinin memnuniyet düzeyini arttıracak şekilde oluşması için üretilen akıllı uygulamalar, teknolojiye bağımlılığı artırdığı gibi aynı zamanda verilere duyulan ihtiyacı da artıracaktır. Bu nedenle verilerin korunmasında her zamankinden daha çok özen göstermek gerekmektedir. Akıllı kentlerde, kentsel hizmet kullanıcılarının verileri, her şeyi akıllı yapmak adına elektronik veri depolama aygıtlarında saklanmaktadır. Bunların en önemli ve en çok kullanılan örneği ise akıllı telefonlardır. Bir sosyal medya uygulaması olan Facebook’un veri sızdırma skandalı bile bu güvenilirliği sorgulatmaktadır (www.cnbc.com, 2019).

**2.2. Dijitalleşmiş Nesnelerin Siber Saldırılara Hedef Olması (Hacklenmesi)**

Hack kelime anlamı olarak eski İngilizce’de “*haccian”* balta veya bıçakla doğramak fiilinden evrilmiştir. Almanca’da da *hakkôn* olarak kullanılan kavramın günümüzde yaygın olarak kullanılan bir başka anlamı ise, “bir bilgisayar sistemine izinsiz girmek”, dijital bir nesnenin, başka bir sistem veya ağa, bu sistemin veya ağın zayıflıkları sonucunda, yetkisiz şekilde sızmasıdır ([www.etimolojiturkce.com](http://www.etimolojiturkce.com), 2019). Sistemlere sızmayı sağlayan bu zayıflıklar; dijital sistem zayıflıkları veya nesnelerdeki zayıflıklar ve insan kaynaklı zayıflıklar olarak sınıflandırılabilir. Hacklenmek ise hackleme işleminden etkilenme durumudur. Hackleme işini yapan kişiler “Hacker” olarak adlandırılmaktadır (ww.tdk.gov.tr, 2019).

Hacklenme işlemi, dijital sisteme yetkisiz kişilerce erişim sağlanıp zarar verilmesine neden olabilmekte veya bu sistemlerde kayıtlı verilerin başka amaçlar için kullanılmasına yol açabilmektedir. Hack saldırısına maruz kalan kişi “kurban” olarak adlandırılmaktadır. Hackerlar, teknik saldırılar dışında sosyal mühendislik (kandırma sanatı) yöntemiyle de kurbanlarını hackleyebilmektedirler. Kaba kuvvet (brute force), sosyal mühendislik, parola kırma, sahtekarlık (spoofing), exploit saldırıları, trojanlar vb. birçok yöntem hackerlar tarafından yaygın şekilde kullanılmaktadır. Bu saldırıları yapanlar üç temel hacker grubu bulunmaktadır [(www.diyalogin.com](http://(www.diyalogin.com), 2019).

a.White Hat (Beyaz-Ak Hackerlar)

b.Black Hat (Siyah Hackerlar)

c.Gray Hat (Gri Hackerlar)

Dijital nesnelerin kötü amaçla hacklenmesi, insanlar, şirketler, kent yönetimleri ve devletlere karşı çeşitli boyutlarda zararların verilmesi amacıyla Siyah Hacker’lar (Black Hat) tarafından gerçekleştirilmektedir. Kişisel veya kurumlara özel verilerin ele geçirilmesi halinde bu bilgilerin kimlik sahtekârlığı için kullanılabilmesi ya da başka kişilere satılabilmesi mümkün olmaktadır. Hacklanme sonucu kötü kişilerce ele geçirilen sistemler üzerindeki dosyalar şifrelenerek fidye istenebilmekte, kişi veya kurumlara ait çeşitli hesaplar ve veri tabanları ele geçirilerek büyük çaplı, olumsuz ekonomik etkiler yaratılabilmektedir ([www.digisophia.com](http://www.digisophia.com), 2019).

**2.3. Siber Suçlar**

Teknolojik gelişmelerle beraber siber suçlarda artmaktadır. Bilişim teknolojisinin gelişmesine koşut olarak giderek büyüyen ve sürekli değişen siber uzay, hukuk normlarının tanımladığı gerçek yaşamda karşılaştığımız birçok suç türüne de ev sahipliği yapmaktadır. Bu suçlar gerçekleştirilirken bilişim sistemlerinin kullanılması veya yardım alınması da siber suçlar olarak tanımlanmaktadır (<http://afyonluoglu.org>, 2019).

Siber suçları bu kadar yaygınlaştıran belli başlı nedenlerin en önemlisi artık internet üzerinde çok değerli kişisel veri kaynaklarının bulunmasıdır. Örneğin; alışveriş, bankacılık, kent bilgi sistemi verileri gibi internet üzerinden verilen servisler kişisel veri kaynakları olarak gösterilebilir. Gerçek para ile internet üzerinde yapılan işlemler, dikkat çekmek amacıyla değil de özellikle kar amacına yönelik çalışan siber suçluların ilgi odağı haline gelmektedir. Dolandırıcılık ve para kazanmak amacıyla işlenen ve suç istatistiklerine giren olay sayılarına bakıldığında 2003 yılında 95 olan olay sayısı, kullanıcı sayısının ve verinin artmasına paralel olarak 2012’de 6718’e yükselmiştir. Bu sayısal artışta bilişim suçları çok büyük bir orana sahiptir (Taşçı ve Can, 2015).

Siber saldırılar karşısında birçok güvenlik türünden söz edilebilir. Bunlar; “[bilgi (istihbarat) güvenliği](http://www.wikizero.biz/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvQmlsZ2lfZyVDMyVCQ3ZlbmxpJUM0JTlGaQ)”,“[bilişim güvenliği](http://www.wikizero.biz/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3cvaW5kZXgucGhwP3RpdGxlPUJpbGklQzUlOUZpbV9nJUMzJUJDdmVubGklQzQlOUZpJmFjdGlvbj1lZGl0JnJlZGxpbms9MQ)”, “[fiziki güvenlik](http://www.wikizero.biz/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3cvaW5kZXgucGhwP3RpdGxlPUZpemlraV9nJUMzJUJDdmVubGlrJmFjdGlvbj1lZGl0JnJlZGxpbms9MQ)”,“[gıda güvenliği](http://www.wikizero.biz/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvRyVDNCVCMWRhX2clQzMlQkN2ZW5saSVDNCU5Rmk)”, “insan can ve mal güvenliği”, “[iş/işçi güvenliği](http://iş/i%C5%9F%C3%A7i%20g%C3%BCvenli%C4%9Fi)”dir ([www.arelzaman.com.tr](http://www.arelzaman.com.tr), 2019).

**III. SİBER SALDIRI SENARYOLARI**

Siber saldırıların sonucunda, akıllı kentlerde çeşitli ölçekte hasarlar ortaya çıkmaktadır. Gerçekleşen siber saldırıların olası sonuçları arasında; siber sistemlerin bir kısmının veya tamamının ele geçirilmesi, veri sızıntısı-dolandırıcılığı, kentin altyapı hizmetlerinin durması veya kesintiye uğraması, enerji kaynaklarının hasara uğratılması, insanların yaşamını tehlikeye sokacak doğrudan zararların ortaya çıkarılması, kentin özel plan veya bilgilerini ele geçirip fidye istemek, sistemleri çökertmek veya etkisiz kılmak sayılabilir.

“Siber ortamdaki sanal veya fiziksel yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken, temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir” (Şenol, 2017: 2).

Güvenlik önlemleri gerektiği gibi olmazsa sonuçlar daha ağır ve beklenilmeyen ölçüde zarara ve hasara neden olabilir. Güvenlik gerektiği şekliyle sağlanamazsa, küçük bir cihazdan bile, ağa dahil olan bütün kentin akıllı sistemleri üzerinde kontrol sahibi olunabilir. Siber güvenlik siber savaşın gelecekte daha fazla önem kazanacağı, uluslararası ilişkilerde güç kontrolünü elinde tutan ülkelerin bunu kullanmaktan çekinmeyeceği uluslararası düzeyde sorunların boyutunun bugünden tahmin edilmesinin güç olduğu çeşitli vesilelerle vurgulanmaktadır. TRT Haber kanalında yayınlanan bir habere göre**, eşgüdümlü olarak gerçekleştirilecek bir siber saldırının olası maliyeti 85-193 milyar dolar olduğu tahmin edilmektedir. Siber** güvenlik suçlarının dünya ekonomisine toplam maliyetinin 2021 yılında ise 6 trilyon dolara ulaşmasının beklendiği belirtilmektedir ([www.trthaber.com](http://www.trthaber.com), 2019).

**3.1. Mobil Cihazlar ve Dijital Platformlar**

Mobil cihazlar (cep telefonu, el bilgisayarı (notebook), Ipad vb.) üzerinden erişilen dijital platform ve uygulamalar, bulundurdukları açıklar nedeniyle saldırılara maruz kalabilmektedir. Akıllı uygulamalarla hizmetlerin yürütüldüğü kentlerde insanlar, yapacakları işleri ve birtakım tercihleri ile ilgili olarak, mobil cihazlarına kuracakları uygulamalarla, saldırganlara veri sızıntısına neden olacak ortam sağlayabilmektedirler. Yöneticilere yönelik olacak bir saldırıda verilerin çalınması, ifşa edilmesi, fidye istenmesine yol açılması, kullanıcı-yönetici yanıltmasına da sebep olabilmektedir. Örneğin, siber saldırıya uğrayan bir toplu taşıma uygulamasında, saldırganlar, seyir halinde olduğu halde birçok aracın servis dışı olduğu bilgisini paylaşabilirler. Bu yanlış bilgi sonucunda şehirdeki binlerce insan kişisel araçlarıyla trafiğe çıkarak trafik yoğunluğunu artırıp, kentin trafik güvenliğini etkileyecek sonuçlara neden olabilir (<http://afyonluoglu.org>, 2019; [https://www.sehirsizin.com](https://www.sehirsizin.com/Documents/Deloitte-Vodafone-Akilli-Sehir-Yol-Haritasi.pdf), 2019)**.**

**3.2. Büyük Veri ve Açık Veri**

Akıllı kentlerde herkese açık çok büyük miktarda veriler bulunmaktadır. Bu veriler kötü niyetli hackerlerinde işine yaramaktadır. Veri koruma ve inovasyon arasında iyi bir denge ayarlanamazsa, insanlarla ilgili konum, zaman ve durum bilgilerini sızdırabilirler. Bu sızdırılan bilgiler terör saldırısı ve siber saldırılara uygun ortam ve bilgi kaynağı olabilir. Terör saldırıları için gereken en uygun duruma, zamana ve mekâna ilişkin bilgiler, açık veriler üzerinden elde edilebilmektedir.

**3.3. Nesnelerin İnterneti**

Nesnelerin interneti kaynağına ulaşmak, herhangi bir siber saldırıda kenti en çok etkileyecek saldırı senaryolarından birisidir. Kentteki elektronik cihazların internete bağlı olarak çalışması nedeniyle gerçekleştirilen bu saldırı az ya da çok etki yaratmaktadır. Örneğin; IoT altyapısıyla idare edilen bir metro, tren hattı, bir siber saldırıya hedef olarak kazalara, büyük felaketlere yol açabilir. İnsanların hayatını kaybetmesine ve devlet araçlarının zarar görmesine neden olabilir. Akıllı enerjiler hacklenerek kentin kaynakları boşa harcanabilir. Bu durum ise hem doğaya hem de kent ekonomisine ciddi zararlar verebilmektedir.

Akıllı kentlerdeki pek çok acil durum veya çözümler, internet üzerindeki duyargalar (sensör) aracılığıyla gerçekleştirilmektedir. Bunlara yönelik bir saldırıda, olmaması gereken gerçek dışı senaryolar yaşanabilir. Saldırganlar olmayan bir sel, deprem, nükleer saldırı gibi afet veya silahlı saldırı alarmları çalarak kentte ayaklanma, panik havası yaratabilirler. Kentteki belediye, polis, vb. gibi ekiplerinin dikkatini başka yönlere çekerek, şehrin güvenlik ve diğer olası risklerini artıracak girişimlerde bulunabilirler.

**3.4. Sosyal Etkileşimli Robotlar**

Akıllı kentlerde birçok hizmetler robotlarla düzenlenmektedir. Kentsel altyapıyı idare eden robotların hizmet üretirken gerek duyduğu kritik verileri depolayan sunucularla olan iletişiminin kesintisiz sağlanması gerekir. Bu robotların bir siber saldırı ile ele geçirilmesi, kentin kritik veri tabanlarına kötü niyetli kişilerin erişimine olanak sağlanmış olacaktır. Bu şekilde elde edilecek bilgilerle altyapı çalışamayacak, sosyal ve ekonomik zararlar ortaya çıkacaktır. Örneğin, yerel yönetimlerde kişisel verilerin toplanmasında kullanılan bir robot, hizmet kullanıcıların kişisel verilerini alıp saldırganlara ileterek, kişisel verilerin güvenliğini zedeleyebilir, kimlik hırsızlıklarına neden olabilir. Diğer bir tehdit olarak da “saldırganların bu robotlarla sosyal mühendislik çalışması yapmadan direkt olarak veri tabanı sunucularından bu bilgileri alarak kolaylıkla farklı saldırılarda kullanması” (<http://afyonluoglu.org>) söylenebilir. Bu dijital robotlar hacklenerek fiziksel birer silaha dönüştürülüp canlı veya cansız kentsel unsurlara zarar verebilirler.

**3.5. İnsansız Araçlar**

Akıllı kent uygulamalarında çeşitli boyut ve içerikte birçok insansız hava ve karasal araç kullanılmaktadır. Bu araçlar kargo, izleme, yolcu taşımacılığı, alarm üretme ve müdahale gibi farklı alanlarda işlev görmektedir. Dolayısıyla bu insansız araçlara yapılacak saldırılar da çok olumsuz sonuçlara yol açabilir. Örneğin; kargo izlemede kullanılan bir aracın siber saldırı yöntemiyle ele geçirilmesi sonucu saldırganlar kargoyu kendi adreslerine yönlendirebilir veya izleme yapan bir araçla bilgi toplayabilir. Yolcu taşımacılığı yapan araçlar ile trafikte kargaşaya neden olup, kente zarar verebileceği gibi insanlara da zarar verebilir, hatta ele geçirilen bu araçlar silahlandırılarak savaş makinesi haline dönüştürülebilir ([http://afyonluoglu.org](http://afyonluoglu.org/), 2019)**.**

**IV. SİBER KORUMA UYGULAMALARI**

Dünyanın birçok modern kentinde uygulanan siber saldırılara karşı güvenlik uygulamaları devletler ve iş dünyası için bir zorunluluk halini almıştır. Herhangi bir metropol kenti güvenli hale getirmek için uygulanması gereken kritik sistemler vardır. Avrupa Birliği’nin Network ve Bilgi Sistemleri’nden sorumlu birimi olan ENISA’daki uzmanlara göre; “akıllı olma yolunda ilerleyen kentlerde siber güvenliğe gösterilen önem halen oldukça düşük seviyelerde seyretmektedir” (http://www.hurriyet.com.tr). Avrupa Birliği uzmanlarına göre, akıllı kentin kullanıcıları arasında siber güvenlik kültürünün yaygınlaştırılması ve altyapısının mutlaka oluşturulması gerekmektedir. Bu kültürün oluşmasında etkili olacak siber güvenlik uygulamaları aşağıdaki şekilde özetlenebilir.

**4.1. Dijital Erişim Kontrol Sistemleri (DEKS)**

Dijital Erişim Kontrol Sistemleri geçerli izni olan kişi veya bölümlerin akıllı kent veri ağlarına erişimine izin veren tek ve mutlak bir prensip üzerine inşa edilmiştir. Erişim serbestisi olan bu kişiler, resmi yetkililer, ilgili şirket ve servis sağlayıcılarının belirlediği görevlilerden oluşabilmektedir. DESK sistemleri, kent servislerini hırsızlık ve saldırı sonucu bozma/zarar verme gibi sonuçlardan koruması açısından yaşamsal öneme sahiptir. Ayrıca bu güvenlik önlemleri, tutarlı ve temiz bir veri erişim tabanı sunarak herhangi bir güvenlik ihlali durumunda yetkilendirilmiş kişilerin sorumluluk seviyelerini belirlemeye de yardımcı olmaktadır. İyi geliştirilmiş bir DEKS, akıllı veri işleme üniteleri ve veri iletim ağları gibi kentin altyapısında yer alan tüm katmanların korunmasını sağlamaktadır.

**4.2. Acil Durum Kurtarma ve Yedekleme Servisleri**

Dijital veri merkezleri, akıllı kentlerden akıllı binalara veya akıllı sokak lambalarından sürücüsüz araçlara kadar IoT’nin sunduğu her şeyin tam kalbinde yer almaktadır. Veri merkezi mimarisinin yaşamsal oluşumu ise “Acil Durum Kurtarma”dır. Çünkü sunucuların çöktüğü durumlarda tüm sistemleri en kısa sürede yeniden çalışır duruma getirmek çok önemlidir. “Yedekleme süreci de en az kurtarma süreci kadar büyük bir öneme sahiptir. Veri yedeklemeleri, daha güvenilir olması amacıyla, düzenli olarak dışarıdan (off site) yapılmalıdır” (<https://tr.nec.com>, 2019).

**4.3. Donanım / Yazılım Hatalarını Gözlemleme**

Bilişim sistemlerinin kullanım durumunun dünden bugüne daha hızlı ve aktif bir şekilde yayılması, bu sistemlerdeki hataların da orantılı olarak artmasına yol açmaktadır. Bu noktada ise devreye donanımlar girmektedir. “…Yakın gelecekte hemen hemen her yerde sensörler, geçitler (gateway), toplayıcılar (integrator), kontrol aygıtları, switchler veya beaconlar gibi donanım aygıtları görülüyor ve kullanılıyor olacaktır” (<http://bestdergisi.com.tr>). Bu denli önem taşıyan bu cihazların ve akıllı kent mimarisinde kullanılan donanımların ve yazılımların herhangi bir siber saldırıya karşı sürekli gözlem altında tutulmasının ve korunmasının sağlanması büyük önem taşımaktadır.

**4.4. Özel Sanal Ağlar**

Özel Sanal Ağlar (Virtual Private Network- VPN) olarak bilinen ağlar, belirli kişi veya grupların kullandığı ağı, herkesin erişebileceği hale getirmeyi sağlamaktadır (www.akillikentler.org). Bu özel ağlar IPsec olarak bilinen ve IoT kent şebekesinin farklı parçaları arasındaki veri alış-veriş halindeki veriler (örneğin; arabayla aydınlatma direği arasında) “kimlik doğrulama”, “yetkilendirme” ve “şifreleme” gibi süreçleri yürüten İnternet Protokol Güvenliği’ni kullanmaktadır. Şifreleme, VPN’lerin sunması gereken en hayati unsurdur. Şifreler ile tüm veri metinleri teoride erişim verilmemiş hiç kimse tarafından anlaşılamayacak bir şifreli metin (cipher-text) haline getirilir. Şifrelemedeki herhangi bir açık veya hata, hackerların paylaşılan bu özel verileri çalmasına olanak tanır ki bu da küçük çaplı bir felaket senaryosuna sebebiyet olabilmektedir.

**4.5. Siber Olaylara Müdahale Organizasyon (SOME) Ekiplerinin Kurulması**

Dijital veri tabanına sahip uygulamaları kullanan bütün akıllı kentlerin, kötü niyetli olası siber saldırılara ve doğuracağı kötü sonuçlara karşı eğitilmiş, bu olaylara müdahale edebilecek nitelikte SOME ekipleri bulundurmaları gerekmektedir. Çünkü olası siber saldırılara karşı nasıl tepki verileceğini, nasıl önlem alınacağını bilmemek, büyük kargaşalara ve olağan kent yaşamının durmasına neden olabilir. Akıllı uygulamalarla yönetilen kentler için ciddi siber güvenlik stratejileri oluşturulması bir zorunluluktur. Alınmakta olan güvenlik önlemlerinin sürekli güncellenmesi ve denetlenmesi gereklidir. Yani saldırılara karşı korunmak isteyenler korsanlardan hep birkaç adım önde olmalıdır. Konunun uzmanlarına göre, olası bir Ddos saldırısında akıllı sistemi yeniden kontrol edip eski haline getirmek, saldırının hangi bölüme yönelik olduğunu analiz etmek, ortaya çıkan hasarın belirlenmesini ve analizini yapmak, saldırıyla ilgili gerekli önlemleri alıp güvenlik açıklarını kapatmak önem arz etmektedir (<https://www.btk.gov.tr>, 2019).

**4.6. DDos/Dos Saldırılarına Karşı Önlem Almak**

Nesnelerin İnterneti (Internet ofThings- IoT) tabanlı sistemler için DDos-Dos saldırılarına karşı önlem almak önem taşımaktadır. IoT tabanlı sistemleri etkisiz hale getirmek için kullanılan yöntemlerden biri de DDos/Dos saldırılarıdır. DDoS saldırıları akıllı kentte kullanılan dijital altyapıyı çökertmek için kolaylıkla kullanılabilecek bir yöntem olarak görülmektedir. Bu nedenle saldırının boyutlarına ve en kötü senaryoya göre; kentin SOME takımı DDoS saldırılarını önlemek üzere etkili bir strateji geliştirmesi ve uygulaması gerekmektedir (Aksoy, 2016). DDos saldırılarını önlemek veya engellemek bulut tabanlı “scrubber” içeren hibrit bulutlar aracılığıyla olabilmektedir (Aksoy, 2016). Olası siber saldırıları önlemek amacıyla alınabilecek diğer önlemler arasında, sistemler için güçlü bir şifrelemenin kullanılması, dışarıdan müdahaleleri önleyecek güçlü korumaya sahip sistemlerin tasarlanması ve manuel (elle) müdahale olanağı sağlanması, aktivitelerin detaylı LOG kayıtlarının tutulması sayılabilir.

**4.7. Siber Güvenlik Akademisi Kurmak**

Son zamanlarda artan hacktivist saldırıların daha hızlı şekilde önlenmesi, zamanında müdahale edilmesi, müdahale edilemese bile hasarının azaltılması için, bilişim sistemlerinde uzman, siber saldırıları çözümleyebilecek, siber stratejileri kurabilecek ve uygulayabilecek, hasar tespiti ve analizi yapabilen, yetenekli insanların acil durumlarda müdahale edebilmesi için eğitilip yetiştirileceği bir akademinin kurulması gereklidir.

**4.8. Akıllı Kentlere Yönelik Siber Saldırı Örnekleri**

Akıllı kentler veya kentlerdeki akıllı uygulamalar, artan siber saldırılarla, teknolojik ilerlemede gösterdikleri çabalara yönelik tehditlerle giderek daha fazla karşı karşıya kalmaktadırlar. 2018 yılından bugüne kadar Atlanta, Baltimore ve SintMaarten Adası’nın, hayati devlet hizmetlerini etkileyen ve bu belediyelerin milyonlarına mal olan geniş çapta çevrimiçi saldırılara maruz kaldığı bilinmektedir. Amerika’nın Atlanta kentinde, 22 Mart 2018 tarihinde bir fideye yazılımı olan SamSAm tarafından sistem zarara uğratılarak kritik görev yazılımlarının % 30’unun hasar görmesine yol açılmış, istenen 55.000 dolarlık bitcoin kent yönetimi tarafından ödenmemiştir. Bu saldırı ile hukuk düzeni açısından çok önemli olan Atlanta’nın on yıllık yasal belgeleri ve polis kamera kayıtları silinmiştir. Bu saldırının maliyetinin 12.2 milyon dolar olduğu açıklanmıştır ([www.dilitrust.com](http://www.dilitrust.com), 2019).

Dünyanın pek çok yerinde siber saldırılara hedef olan akıllı kent uygulamaları söz konusudur. Bunlardan bazıları dünyada siber saldırı örnekleri başlığı altında belirtilmiştir.

**4.9. Dünyada Siber Saldırı Örnekleri**

* 23 Aralık 2015 Ukrayna: Enerji istasyonlarına yapılan siber saldırıdan dolayı 230.000 kişinin elektriği kesilmiştir ([www.hurriyet.com.tr](http://www.hurriyet.com.tr), 2018).
* 4 Kasım 2016 İsveç: İsveç’te Hava Trafik Kontrol Sistemi hacklenmiştir. Bundan dolayı 1 günlüğüne yurt içi ve dışı tüm uçuşlar iptal edilmiştir (<https://siberbulten.com>, 2019).
* 7 Nisan 2017 Dallas-Amerika: Hackerlar saat 11.40’ta 156 acil yardım sirenlerini aktif hale getirip halkta gerginlik sağlamıştır. Sirenler saat 1.20’de ancak kapatılmıştır. O gün içerisinde 911’e 4.400 tane arama yapılmıştır (<https://ioactive.com>, 2019).
* 18 Kasım 2017 Sacramento: Bir fidye yazılımı 30 milyon dosyayı silmiş ve saldırganlar 7000 $ Bitcoin cinsinden talep etmiştir ([www.cnbc.com](http://www.cnbc.com), 2019).
* Mart 2016 Undisclosed City: Su Arıtma Sistemleri aracılığıyla saldırganlar suyu arıtmak için kullanılan kimyasalların seviyelerini değiştirerek 2,5 milyon müşterinin verilerini çalmışlardır (<https://ioactive.com>, 2019).
* 25 Kasım 2016 San Francisco: Belediye demiryolu sistemine fidye yazılımı bulaşmış ve en az 100 Bitcoin fidye istenmiştir ([www.cnbc.com](http://www.cnbc.com), 2019).
* 11 Ekim 2017 İsveç: Ulaşım yönetimi sistemlerine Ddos saldırısı gerçekleştirilmiş ve tren izleme sistemlerine saldırılmıştır. Ayrıca bu saldırı federal ajansın e-posta sistemini, web sitesini ve yol trafik haritalarını da etkilemiştir. Trafik yönetimi ve diğer hizmetlerin yedekleme işlemleri elle yapılmak zorunda kalınmıştır. Bazı trenler durmuş ve binlerce yolcuyu etkileyen gecikmeler yaşanmıştır (<https://siberbulten.com>, 2019).
* 31 Mart 2015 Türkiye: Siber saldırı sonucunda Türkiye genelinde en az 40 ilde Elektrik kesintisi yaşanmıştır (<http://dergipark.gov.tr>, 2019).
* 21 Mart 2016 İstanbul: Ekber Was Here: [Sabah](http://www.milliyet.com.tr/sabah/) saatlerinde [İstanbul](http://www.milliyet.com.tr/istanbul/) Elektrik Tramvay ve Tünel İşletmeleri Genel Müdürlüğü’nün ([İETT](http://www.milliyet.com.tr/iett/)) internet sitesinin siber saldırıya uğraması sonucu İstanbul’daki toplu taşıma araçlarının ekranlarında ‘[Ekber was here](http://www.milliyet.com.tr/ekber-was-here/)’ yazıları görülmüştür. Bu tarihte 07.20 - 09.00 saatleri arasında, İETT'nin internet sitesine de erişim sağlanamamıştır ([www.milliyet.com.tr](http://www.milliyet.com.tr), 2016).
* 2017 Xian-Çin: Trafik lambalarının bozulması sonucu oluşan  trafik sıkışıklığı, Xi’an, Çin korsanların akıllı trafik lamba sistemlerini ele geçirmesi bu tür kargaşalara sebep olmuştur (<http://www.win-eurasia.com>, 2019).
* 19 Şubat 2013 Çongçing: Çin’in en büyük beşinci şehri Çongçing’de bulunan Yangrenjie Eğlence Parkı’ndaki trafik ışıklarının aynı anda hacklenmesi yine trafik sorunu yaşanmasına neden olmuştur ([www.dilitrust.com](http://www.dilitrust.com), 2019; <http://www.milliyet.com.tr>, 2019)**.**

**SONUÇ**

Kentsel hizmetlerin ve kentsel altyapının, daha iyi hizmet sunmak üzere, gelişen teknolojinin olanaklarından yararlanarak akıllı uygulamalarla donatılması bir gereklilik haline gelmiştir. Bilgisayar ve internetle birlikte toplum yaşamının her alanına giren bilişim teknolojisi, kent ve mekânla uyumlaştırılarak, insanların yaşam biçimlerini ve alışkanlıklarını değiştirmekte, kolaylaştırmakta veya insanları buna zorlamaktadır.

Kentsel altyapıda ve diğer hizmetlerde bilişim teknolojisinin kolaylıklarından ve olanaklarından yararlanmak iyi sonuçlar doğuruyor olsa da, birer bilişim yazılımı sistemi tabanıyla gerçekleştirilen kentsel düzenlemeler, dijital tehditlere karşı da açık durumdadır. Küreselleşme bilginin erişimini kolaylaştırdığı gibi kullanım risklerini de aynı oranda artırmaktadır.

Günümüzde küreselleşmenin ve dijital teknolojinin etkisiyle bilgiye erişimin kolaylaşması, kent yönetiminde de yeni bir rekabet sistemi oluşturmuştur. Bu sistem kentsel mekânda yaşanılabilirliği artırmayı ve teknolojik imkanlardan daha fazla yararlanmayı sağlayacak dijital altyapı yazılımlarının kurulmasını teşvik etmektedir. Ancak bu yazılımların gelişmiş ülkelerin büyük yazılım firmaları eliyle gerçekleştiriliyor olması, yeni bir bağımlılık alanı yaratmaktadır. Bu şirketlerin kurduğu altyapılara yönelik tehditlerin önlenmesi ve giderilmesi noktasında da yine bu şirketlerin ürünlerine ihtiyaç duyulması bir başka bağımlılığı beraberinde getirmektedir. Eğer bir ülke teknolojinin üreticisi değil, sadece kullanıcısı durumunda ise teknolojik kullanımdan doğan riskleri de kabul etmek zorunda kalmaktadır. Bu da çok uluslu şirketlere ve gelişmiş ülkelere bağımlılığı artırtmaktadır.

Kapitalizmin yeni karlılık alanı olarak hayatımıza giren akıllı kent uygulamalarının kentsel hizmetlerde getirdiği kalite ve hız tartışmasız yaşam kalitesini artırmaktadır. Ancak bu uygulamaların yazılım altyapısının yerli teknolojiler tarafından yapılması için gereken çabanın da gösterilmesi gereklidir. Aksi halde dışa bağımlılık ve siber tehditler karşısında savunmasızlık her an için söz konusu olacaktır. Her geçen gün siber uzay ile ilgili yeni bir gelişmeye tanık olunurken, akıllı sistemlerin kentsel mekâna uygulanması kadar korunması konusunda da duyarlılık gösterilmesi gerekmektedir.

**KAYNAKÇA**

# Aksoy, D. (2016), Akıllı Şehirlerde Siber Saldırıları Önlemek, Global-Tech Magazine.

Çelik, S. (2018), Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım, *Academic Review Of Humanities And Social Sciences*, 1(2), 110-119.

Washburn, D. and Sindhu, U. (2011), “Helping CIOs Understand “Smart City” Initiatives, Forrester, February,11.

Goychayev, R, Clements, S. L.,McKinnon, A.D, Carr, G.A., Benz, J. M, Andres, R. B., Weise, R.A, Rodda, K.E., Donnelly, D.A.,and Bartholomew, R.A. (2017), Cyber Deterrence and Stability Assessing Cyber Weapon Analogues Through Existing WMD Deterrence and Arms Control Regimes, September <https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26932.pdf> (Erişim Tarihi: 20.01.2019)

Kut, S. (2013), Sibertektonik Mekân, Yayınlanmamış Doktora Tezi, İTÜ Fen Bilimleri Enstitüsü, İstanbul.

Stratigea, A. (2012), The Concept of “Smart Cities”. Towards Community Development? NETCOM Networks and Communication Cities, 26 (3/4), 375-388.

Şenol, M. (2017), Türkiye’de Siber Saldırılara Karşı Caydırıcılık, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3 (2), 1-9.

Taşcı, U. ve Can, A. (2015), Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014, *Fırat Üniversitesi Sosyal Bilimler Dergisi,* 25 (2), 229-248.

Uçar, A., Şemşit, S. ve Negiz, N. (2017), Avrupa Birliği Kent Uygulamaları ve Türkiye’deki Yansımaları, *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 22, Kayfor 15 Özel Sayısı, 1785-1789.

Velibeyoğlu, K. (2016), “Akıllı Kentler: Vaatler ve Ötesi”, Yenilikçi Sürdürülebilir Gelişme Stratejileri Bağlamında Türkiye Ekonomisinin Geleceğine Yönelik Çözüm Arayışları içinde, Editör: Şanlısoy, S., DEÜ İktisat Bölümü, İlkim Ofset ve Dijital Baskı Sistemleri, İzmir.

Yılmaz, E. ve Çitçi, S. (2011), Kentlerin Ortaya Çıkışı ve Sosyo- Politik Açıdan Türkiye’de Kentleşme Dönemleri, E*lektronik Sosyal Bilimler Dergisi*, 10 (35), 252-267, [www.esosder.org](http://www.esosder.org) (Erişim Tarihi: 10.02.2019).

Kişisel Verinin Korunması Kanunu, Resmi Gazete 07.04.2016 Tarih ve 29677 Sayı, [www.resmigazete.gov.tr](http://www.resmigazete.gov.tr) (Erişim Tarihi: 10.03.2019).

<https://www.dilitrust.com/en/blog/cyber-attacks-smart-cities/> (Erişim Tarihi: 10.03.2019).

<https://www.emlaksayfasi.com.tr/guncel/2025-yilina-kadar-turkiye-de-26-akilli-kent-olusacak-h25620.html> (Erişim Tarihi: 10.03.2019).

<https://journals.openedition.org/netcom/1105>, (Erişim Tarihi: 21.02.2019).

<http://www.arelzaman.com.tr/kamera-sistemleri> (Erişim Tarihi: 23.01.2019).

<http://www.win-eurasia.com/tr/akilli-sehirlerin-siber-guvenligi> (Erişim Tarihi: 12.02.2019).

<http://www.milliyet.com.tr/cin-de-trafik-lambasi-kaosu-gundem-1670524/> (Erişim Tarihi: 22.03.2019).

<https://www.endustri40.com/akilli-sehirlerin-siber-guvenligi/>(Erişim Tarihi: 09.04.2019).

<http://www.hurriyet.com.tr/teknoloji/turkiyenin-siber-kalkani-ahtapot-yayginlastirilacak-41065234> (Erişim Tarihi: 02.02.2019).

<http://bestdergisi.com.tr/arsiv-eski/118-akilli-kentler-icin-iot-siber-guvenlik-uygulamalari/> (Erişim Tarihi: 13.04.2019).

<https://www.btk.gov.tr/haberler/siber-guvenlik-akilli-sehirlerin-vazgecilmezidir> (Erişim Tarihi: 11.04.2019).

<https://tr.nec.com/tr_TR/global/solutions/safety/index.html> (Erişim Tarihi: 18.04.2019).

<https://www.sehirsizin.com/Documents/Deloitte-Vodafone-Akilli-Sehir-Yol-Haritasi.pdf> (Erişim Tarihi: 23.02.2019).

<http://www.diyalogin.com/hacker-saldiri-yontemleri/> (Erişim Tarihi: 23.03.2019).

<https://emoji.com.tr/siber-saldiri-nedir/> (Erişim Tarihi: 12.03.2019).

<https://www.globaltechmagazine.com/2016/12/23/akilli-sehirlerde-siber-saldirilari-onlemek/> (Erişim Tarihi: 11.03.2019).

<https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> (Erişim Tarihi: 01.03.2019).

<https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf> (Erişim Tarihi: 03.02.2019).

[http://afyonluoglu.org](http://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/2018-Ozgur%20Alp_Ak%C4%B1ll%C4%B1%20%C5%9Fehirlerde%20siber%20g%C3%BCvenlik.pdf) (Erişim Tarihi: 11.01.2019).

<https://www.etimolojiturkce.com/kelime/hack> (Erişim Tarihi: 30.01.2019).

[www.tdk.gov.tr](http://www.tdk.gov.tr) (Erişim Tarihi: 10.02.2019).

<http://www.digisophia.com/article/details/34> (Erişim Tarihi: 23.03.2019).

<http://www.akillikentler.org/detay/3086/6/akilli-kentler-icin-iot-siber-guvenlik-uygulamalari.html> (Erişim Tarihi: 11.04.2019).

<https://www.haberturk.com/abd-2016-baskanlik-secimleri-nde-rus-siber-saldirisinin-izleri-ortaya-cikarildi-2058952-ekonomi> (Erişim Tarihi: 11.04.2019).

<https://www.trthaber.com/haber/bilim-teknoloji/dunya-6-trilyon-dolarlik-siber-saldiri-riskine-karsi-hazirlaniyor-408564.html> (Erişim Tarihi: 15.03.2019).

<https://www.globaltechmagazine.com/2016/12/23/akilli-sehirlerde-siber-saldirilari-onlemek/> (Erişim Tarihi: 15.03.2019).

<https://siberbulten.com/siber-saldirilar-2/ddos-saldirilari-isvecte-trafigini-etkiledi/> (Erişim Tarihi: 15.03.2019).

<http://www.hurriyet.com.tr/teknoloji/ukraynada-elektrik-dagitim-sistemi-siber-saldiriya-ugradi-40043686> (Erişim Tarihi: 25.02.2019).

<https://www.cnbc.com/2018/11/21/hacker-lifts-1-million-in-cryptocurrency-using-mans-phone-number.html> (Erişim Tarihi: 25.02.2019).

1. \*\* \*Bu çalışma, 18-20 Nisan 2019 tarihleri arasında Gaziantep’te düzenlenen 13. Uluslararası Kamu Yönetimi Sempozyumu’nda sunulan çalışmanın genişletilmiş halidir.

 Doç. Dr., Bayburt Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü, hsengun@bayburt.edu.tr, ORCID: https://orcid.org/0000-0002-1899-8329 [↑](#footnote-ref-1)
2. \*\*\* Abdülsamet KOÇHAN, Öğrenci, Bayburt Üniversitesi İİBF Siyaset Bilimi ve Kamu Yönetimi Bölümü, redlin3q@gmail.com [↑](#footnote-ref-2)
3. \*\*\*\* Dr. Öğr. Üyesi, Yozgat Bozok Üniversitesi, MMF Şehir ve Bölge Planlama Bölümü, secil.meydan@bozok.edu.tr, ORCID: https://orcid.org/0000-0001-9869-4159 [↑](#footnote-ref-3)