Asya Studies
Academic Social Studies/Akademik Sosyal Araştırmalar
DOI: 10.31455/asya.537197 / Number: 7, p. 71-78, Spring 2019

GÖKLERDEKİ EGEMENLİĞE BİLGİSAYAR SİSTEMLERİNİN YANSIMALARININ İNCELENMESİ

INVESTIGATION OF THE REFLECTIONS OF COMPUTER SYSTEMS IN THE SKILLS

Araştırma Makalesi / Research Article

Makale Geliş Tarihi / Article Arrival Date
08.03.2019

Makale Kabul Tarihi / Article Accepted Date
31.03.2019

Makale Yayın Tarihi / Article Publication Date
31.03.2019

Asya'dan Avrupa'ya Uluslararası Sosyal Bilimler Dergisi

Emel Şahin
Muğla Sıtkı Koçman Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler- Yüksek Lisans Öğrencisi
53emelsahin@gmail.com

ORCID ID
https://orcid.org/0000-0001-7194-6758

Öz

Savaş alanlarının karadan havaya taşınması ile Hava Kuvvetlerine, dolayısıyla uçaklara, önem artmış ve her geçen gün artmaya devam etmektedir. Uçaklar sadece havadan yapılacak saldırılar için önem taşımamakta, aynı zamanda 'gökyüzünde göz' olarak üst düzey incelemeler sağlamaktadır. Türkiye'nin kurucusu olan Mustafa Kemal Atatürk de gökyüzüne önem vermiş ve verdiği önemi en net olarak 'İstikbal Göklerdedir.' sözü ile ortaya koymuştur. Ancak zamanla internetin ve bilgisayar sisteminin gelişmesi ile oluşan siber alan, çoğu alanda olduğu gibi güvenlik alanlarında da yeni tehditler ortaya çıkarmıştır. Olusan veni güvenlik tehditlerinden hava sistemleri de etkilenmiştir. Teknoloji dünyasından savaş alanlarına da sıçrayan siber saldırılar yüzünden artık bir uçağın bilgi sistemi, bir bilgisayar tarafından ele geçirilebilecek hale gelmiştir. Bir bilgisayarın bu denli uçak sistemini ele geçirdiği günümüz dünyasında istikbalin hala göklerde olduğu düşüncesi de doğal olarak değişim göstermektedir.

Bu çalışmanın temel hipotezi, İstikbalin artık göklerdeki hava kuvvetlerinden çok bilgisayar sistemlerine olan hakimiyette olduğu düşüncesidir. Çalışmanın doğru şekilde analiz edilmesi için siber dünyanın gelişmesi ile bilgisayar sistemlerinin uçak sistemlerini nasıl etkilediği araştırılmıştır. Bu çalışmada siber uzay çerçevesinde uçaklara yapılan saldırı örnekleri incelenmiştir. Çalışmada verilen örnekler, çalışmanın hipotezini doğrulayacak niteliktedir. Çalışmada elde edilen bulgulardan yola çıkarak siber alanın uçak sistemleri için birçok yeni tehdit oluşturduğu sonucuna varılmıştır. Bu çerçevede siber alanın getirdiği tehditler dikkate alınarak gerekli tedbirler alınması gerekmektedir. Çalışmada, uçaklara yapılan siber saldırıların konu olduğu uluslararası platformlara da değinilmiştir. Çalışmanın amacı yaşanan siber tehditlerden ve örneklerden yola çıkarak siber alanın uçak sistemlerindeki etkisini gözler önüne sermektir. Çalışmanın sonuç kısmında hava sistemlerine yapılan siber saldırılar için önerilere yer verilmiştir. Araştırmanın yöntemine değinecek olursak, çalışmada nicel yöntemler kullanılmıştır. Çalışmanın siber alan konusunda daha sonra yapılacak olan çalışmalara katkı sağlaması ümit edilmektedir.

Anahtar Kelimeler: Siber Saldırılar, Uçak, İstikbal, Bilgisayar Sistemleri, Egemenlik.

Abstract

With the transfer of the battlefields from the land to the air, the importance of the Air Force, and therefore of the aircraft, has increased and continues to increase day by day. Airplanes are not only important for airborne assaults, they also provide high-level inspections as ım eyes in the sky. Turkey's founder, Mustafa Kemal Ataturk, who also gave attention to the importance of the clearest skies and give it as 'Future is in the heavens.' revealed by the word. However, over time, the cyber space that emerged as a result of the development of the Internet and the computer system, as in most areas, has also created new threats in the security fields. Air systems were also affected by new security threats. Because of the cyber attacks that spread from the world of technology to the battlefields, the information system of an airplane has become capable of being captured by a computer. The idea that the future is still in the skies is changing naturally in a modern world where a computer seizes this kind of aircraft system.

The basic hypothesis of this study is that the Istikbal is now dominated by computer systems rather than by air forces in the sky. In order to analyze the study correctly, the development of cyber world and how the computer systems affect the aircraft systems were investigated. In this study, the samples of the attack on the aircraft in the framework of cyber space were examined. The examples given in the study can confirm the hypothesis of the study. Based on the findings of the study, it was concluded that the cyber area posed many new threats to aircraft systems. In this context, it is necessary to take necessary measures to take into account the threats of the cyber area. In this study, the international platforms where cyber attacks on aircraft are the subject are also mentioned. The aim of the study is to reveal the effects of cyber space on aircraft systems based on the cyber threats and examples. In the conclusion of the study, recommendations for cyber attacks on air systems are included. In the study, quantitative methods were used in the study. It is hoped that the study will contribute to the future workes on cyber space.

Key Words: *Cyber Attacks, Aircraft, Istikbal, Computer Systems.*

Citation Information/Kaynakça Bilgisi

Şahin, E. (2019). Göklerdeki Egemenliğe Bilgisayar Sistemlerinin Yansımalarının İncelenmesi. *Asya Studies-Academic Social Studies/Akademik Sosyal Araştırmalar,* Number:7, Spring, p. 71-78.

GİRİŞ

Türk Dil Kurumu sözlüğünde: "Alışılmış kalıpların dışında yeni fikir akımları, kuram[1]" olarak tanımlanan teori, Uluslararası İlişkileri sistematik bir çerçevede ele almayı sağlayan düşünce sistemidir. Uluslararası İlişkilerde tarih boyunca birçok teori ortaya atılmış ve atılmaya devam edecektir. Bu ortaya atılan teorilere zamanla jeopolitik teorilerde eklenmiştir.

Bu zamana kadar jeopolitiğin tanımıyla ilgilenen bilim adamları şu üç kelimeyi mutlaka kullanmışlardır: Devlet, coğrafya ve politika. Bu üç kelimeden oluşacak her türlü tanımlama jeopolitiği açıklamak için yeterli olacaktır. Fakat bunlardan bir tanesinin eksik olması jeopolitiği eksik kılmaktadır[2].

Tarih boyunca hem ülkelerin güvenlikleri için hem de dünya hakimiyeti için ortaya atılan jeopolitik teoriler farklı şekilde temellendirilmiştir. Mackindir odak noktası olarak karayı seçip, Kara Hakimiyeti Teorisi'ni ortaya atarken; Alfred T. Mahan temelini deniz üzerinden kurmuş ve Deniz Hakimiyeti Teorisi'ni ortaya atmıştır. Havacı olan Albay Havsy Scitaklian ise, 'Havaya hükmeden bir milletin dünyaya da hükmedeceği' düşüncesi ile Hava Hakimiyeti Teorisi'nin temellerini ortaya atmıştır. Hava Hakimiyeti Teorisi'nin uygulanması, Birinci Dünya Savaşı ile başlamış ve günümüzdeki bölgesel savaşlarda devam etmektedir [3].

Mustafa Kemal Atatürk'ün de Hava Hakimiyeti Teorisini destekler nitelikte söylemleri bulunmaktadır. 1 Kasım 1924 yılındaki Türkiye Büyük Millet Meclisi açılış konuşmasında: "Yurt savunmasından söz ederken, askeri alanda önemli ve etkin bir nitelik taşıyan hava kuvvetlerine, yüce Meclis'in özellikle ilgi ve dikkatini çekerim." sözü ve daha sonraki konuşmasında ifade ettiği "Göklerini koruyamayan uluslar, yarınlarından asla emin olamazlar." sözü Atatürk'ün göklere verdiği önemi ortaya koymaktadır. Bunun en net kanıtı da Atatürk'ün ifade ettiği "İstikbal Göklerdedir" sözü ortaya koymuştur[4]. Savaşların ve stratejilerinin daha çok deniz ve kara üzerinden yapıldığı o dönemde Atatürk'ün havaya verdiği önem onun ileri görüşlü bir deha olduğunu bir kere daha kanıtlamaktadır.

Bu bağlamda, bu araştırmada, öncelikle uçakların gelişiminden bahsedilmiş daha sonra uçaklara yapılan siber saldırı örneklerine değinilmiş ve uçaklara yapılan siber tehditlerin konu olduğu uluslararası platformlardan bahsedilmiştir. Ayrıca çalışma, teknolojinin gelişmesi ile siber alanın hava hakimiyetine nasıl etkilerde bulunduğunu ele alarak alınması gereken önlemleri ortaya koymaktadır.

1. Uçakların Gelişimi

Uçak 1903 yılında Wright kardeşlerin çalışmaları sonucunda bulunmuştur[5]. Fakat uçakların bir savaş aracı olarak görülmesi Birinci Dünya Savaşında olmuştur. Savaşın gidişatını önemli ölçüde değiştirdiği için Birinci Dünya Savaşı bitiminden sonra da uçaktaki gelişmeler son hızla devam etmiştir. İkinci Dünya Savaşı'nda da uçakların neler yapabileceğini herkes tarafından görülmüştür[6].

Savaş Uçakları yaklaşık yüzyıllık bir maceranın ardından bugünkü halini almıştır. Uçaklar sadece havadan yapılacak saldırılar için önem taşımamakta aynı zamanda gökyüzünde üst düzey incelemeler sağlamaktadırlar. Tarih boyunca savaş uçakları; 2003 yılında Ortadoğu çöllerinden 1914 yılında Fransız siperlerine kadar pek çok kilit görev üstlenmiştir[7].

Ancak gelişen konjonktürde savaş uçakları eskisi kadar önem arz edemez hale gelebilir. Peki bunun sebebi nedir? Yirminci yüzyılda, insanoğlunun aydaki adımlarıyla başlayan ve internetin keşfiyle devam eden Bilgi Devrimi dünyadaki tüm sınırları ortadan kaldırmış, dünyanın dengelerini değiştirmiştir ve siber dünya denilen yeni bir sanal dünya oluşturmuştur. Her geçen gün gelişen siber alan sayesinde günümüzde internetin olmadığı bir alan neredeyse kalmamıştır. İnternetin bu şekilde hayatımıza nüfuz etmesi yeni tehlikeleri ve tehditleri de ardından getirmiştir. Son yıllarda sayısı oldukça artan siber saldırılar da belli başlı saldırı türleri kullanılmaktadır. Aşağıda ki tabloda 252 şirket tarafından ölçülerek elde edilen veriler bulunmaktadır[8].

---

[1]Türk Dil Kurumu ,1960, http://www.tdk.gov.tr/index.php?option=com_bts&view=bts&kategori1 =veritbn&kelimesec=309540 adresinden 01.01.2019 tarihinde erişildi.

[2]İsmail Hakkı İşcan; Uluslararası İlişkilerde Klasik Jeopolitik Teoriler ve Çağdaş Yansımaları, *Uluslararası İlişkiler Akademik Dergi*, C.1, S.2, Ankara, 2004, s. 50.

[3]Çağdaş Duman*; Jeopolitik Teoriler*, İstanbul, 2018.

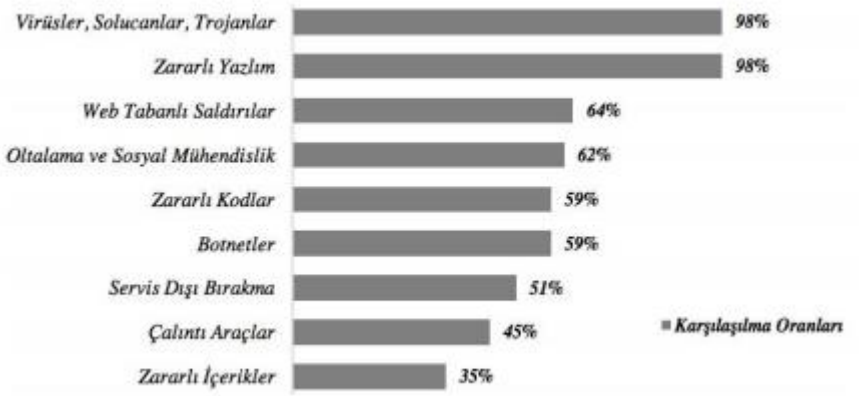
[4]Muhterem Erenli, Atatürk ve Havacılık, http://www.atam.gov.tr/dergi/sayi-04/ataturk-ve-havacilik/ adresinden 01.01.2019 tarihinde erişildi.

[5]Uçak Nasıl İcat Edildi, http://www.airportturk.net/ucak-nasil-icat-edildi.html/ adresinden 01.01.2019 tarihinde erişildi.

[6]Uçağın İcadı ve Tarihsel Gelişimi, 2015, http://merkurbilet.com/blog/ucagin-icadi/ adresinden 01.01.2019 tarihinde erişildi.

[7]Tomtaş Fatih Dervişoğlu; İstikbalini Göklerde Arayan Ülke Ve Türk Havacılık Sahasında Alman Menfaatleri Işığında Bir Ortaklık, *Cumhuriyet International Journal of Education-CIJE*, S.3, Sivas, 2014, s. 68-82.

[8]Vahit Güntay; Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler, *Güvenlik Stratejileri* , S. 27, İstanbul, 2014, s.84-85.



Grafik 1. Siber Saldırı Türlerinin Karşılaşılma Sıklığı[9]

Grafikte de görüldüğü üzere siber alan kendine saldırı için birçok tür bulmuştur. Teknolojinin gelişmesi ile bu türlerin çoğalması muhtemeldir. Dolayısıyla türlerin çoğalması siber saldırı ve tehditlerin çoğalmasına yol açacaktır.

Artan siber saldırılardan dolayı hava sistemi ve uçaklar da yeni gelen tehlike ve tehditlere maruz kalmışlardır. Teknolojinin gelişmesiyle oluşan siber alan sayesinde uçakların bilgi sistemlerine sızıp uçağın tüm kontrol mekanizmasının bir hackerın eline geçmesi hayal olmaktan çıkmıştır. Uçağın pilotun kontrolünden çıkıp bilgisayar başında herhangi birinin kontrol mekanizması haline gelmesinin sonuçları oldukça ağır olabilir.

Mesela, Fly-by-wire manüel uçuş kumandalarını elektronik bir ara yüz ile değiştiren gelişmiş uçuş kumanda sistemidir. Bu sistemde uçak pilottan bağımsız bilgisayar kontrollü basit bir yapay zekaya sahiptir[10]. Peki siber saldırıların bu kadar arttığı günümüzde bu kumanda sistemi yeterince güvenli midir?

Ya da askeri, sivil (hobi ve ticari) ve bilimsel amaçlı profesyonel kullanımları, hem ülkemizde hem de dünyada, hızla artan insansız hava araçlarının siber güvenlik açısından risklerinin olduğunun iddia edilmesi dikkate alınması gereken bir konudur. İnsansız hava araçlarının yakın bir tarih de yaygın kullanım göstermesi ile beraber hava trafiğinde internet bazlı hava trafik kontrolünün yapılması siber saldırı olasılığını arttırabilir. İnsansız hava araçların da kullanılan, Otomatik Bağımlı İzleme (ADS-Automatic Dependant Surveillance) sisteminin siber güvenlik açısından saldırıya açık olduğu iddia edilmektedir. Olası muhtemel güvenlik sorunları, enformasyon ve bilgi teknolojileri üzerinde araştırmalar yapan uluslararası bir kuruluş olan EURECOM tarafından ortaya konmuştur[11]:

-Kimlik doğrulama eksikliğinden dolayı kaynağı bilinmeyen kişilerce yapılabilecek olan yerleştirme mesajlardan korunma sorunu,

-Mesaj doğrulama kodu veya imzası eksikliğinden dolayı mesajlar üzerinde çeşitli değişiklik yapabilme veya belirli bir uçaktan gönderiliyormuşçasına veri akışı sağlanmasına karşı korunma sorunu,

-Mesaj şifreleme eksikliğinden dolayı oluşabilecek gizli dinlemeye karşı koruma sorunu,

-Özel bilgi girişi yoluyla sağlanmaya çalışılan korumanın sürekli ataklara karşı yetersiz kalabilme sorunu,

-Tanımlama sistemlerinin kısa ömürlü hafızalarının özel bilgi takip etme ataklarına karşı etkisiz kalabilme sorunu.

Bu maddeler insansız hava araçlarının karşılaşacağı sorunsallardır. Ayrıca, söz konusu sistemle uçak dünyanın neresinde olursa olsun pozisyon, hız, irtifa, baş açısı ve yapmak istediği manevrası ile ilgili bilgiler otomatik olarak uydu veya diğer haberleşme veri hatları vasıtasıyla siber saldırı

[9]Ponemon Institute, 2015 Cost of Cyber Crime Study: Global, Ponemon Institute Research Report, Michigan, 2015, s. 11.
[10]Fly-by-wire, http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3 dpa2kvRmx5LWJ5LXdpcmU adresinden 02.01.2019 tarihinde erişilmiştir.
[11]Hasan Karakuş; Sivil Havacılık Sektörü ve Siber Güvenlik; İnsansız Hava Araçları Örneği, Erciyes Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi, Yayınlanmamış Lisans Tezi, Erciyes, 2017, s.24.

gerçekleştirecek olan hackerların eline geçebilir[12]. İran tarafından ele geçirilen ABD'nin Lockheed Martin RQ-170 Sentinel isimli İnsansız Hava Aracı ve Nasa'ya ait olan İnsansız Hava Aracının bazı kişiler tarafından hacklenmesi buna örnektir.

Başka bir konu da uçakların radar sistemleri olan A-SMGCS (Advanced-Surface Movement Guidance and Conrtol Systems), uçakların ve bazı araçların anlık hareket bilgilerini sunmaktadır. Gelişmiş siber saldırı türleri ile uçağın radar sistemine girilip bilgi alınabilir ya da yönlendirme yapılabilir. Ayrıca bu bilgilere virüs sayesinde kesinti yapılması her şeyi dondurmaya sebep vererek zincirleme bir aksaklık yaratabilir [13].

Dolayısıyla gerek uydularla konum belirleme sistemlerinin gerekse bu sistemlere önemli ölçüde bağlı olan insansız hava araçları olmak üzere ilgili tüm sistemlerin siber saldırıya maruz kalma olasılığının yüksekliği söz konusudur. Bu da artık uçakların sahip olduğu egemenliğin bilgisayar sistemlerine doğru kaydığının göstermektedir.

2. Uçaklara Yapılan Siber Saldırı Örnekleri

Bazı siber saldırı örnekleri üzerinden gidersek: Tek pilot ve tek motorlu, beşinci nesil, hava-yer taarruz, keşif, taktik savunma gibi çok maksatlı görevleri ve düşük görünürlük özelliğine sahip olan F35 taarruz uçağına[14] yönelik bir siber saldırı gerçekleştirilmiştir. Kasım 2016'da, dünyanın beklediği ve Türkiye ile 8 ülkenin ortak projesi olan F35 savaş uçağının bilgilerinin hacklendiğinin ortaya çıkması yeni soruları da beraberinde getirmiştir. Hacker'ların F35 savaş uçakları için ürettiği elektronik radar sistemiyle ilgili gizli bilgilere ulaştığı iddia edilmiştir[15]. Yapılan bu siber saldırı örneği, günümüzde savaş veya çatışma sırasında üstünlük sağlayacak olan F35 savaş uçağının, bilgisayar ile yapılan bir siber saldırıya maruz kalabildiğini göstermektedir. Teknoloji harikası olarak geçen F35 savaş uçağına bu denli bir saldırı gerçekleşmesi bilgisayar sistemlerinin önemini gözler önüne sermektedir.

Başka bir örnek ise havacılık devi olarak anılan ve dünyanın en büyük sivil ve askeri uçak ve helikopter üreticilerinden olan Boeing'e yapılan siber saldırı ile ilişkilidir. Boering, WannaCry olduğuna inanılan kötü amaçlı bir yazılım virüsü tarafından 2018 yılında saldırıya uğramıştır. Boering sözcüsü Mills, "Siber güvenlik operasyon merkezimiz, sistemlerimizin bir kısmını etkileyen kötücül yazılım keşfetti. Gerekli iyileştirmeler yapıldı" ifadelerini kullanmıştır. Ayrıca bu virüsün, uçak devinde büyük bozulmaya neden olabileceği açıklanmıştır[16]. Dolayısıyla uçak devrine zarar verebilecek kapasiteye sahip olan bir virüs, bir çatışma veya operasyon sırasında uçağın işlevlerini devre dışı bırakabilir. Böyle bir olasılık da uçağın sağlayacağı avantajları bir anda dezavantaja döndürebilir.

Ayrıca, United Airlines Amerikan siber güvenlik kuruluşu Arbor'un endüstriyel casusluk saldırısı olarak nitelendirilen saldırıya hedef olmuştur. FBI kaynaklarına göre, Mayıs 2015'te bir bilgisayar güvenlik uzmanı bir yolcu uçağının kabin içi eğlence sistemine sızmış ve motorların birine tırmanış moduna geçme komutu vererek uçağı kısa bir süreliğine yanlamasına uçurmuştur. Bu olay, bir hacker'ın uçuş sırasında bir uçağın kontrolünü eline geçirdiği ilk örnektir[17]. Bu olay uçaklarda ki güvenlik açıklarını da ortaya koymaktadır. Burada bilişim ve ağ uzmanlarının da son dönemde odaklandığı tartışma konularından biri olan 'Uçaklar hackerlenebilir mi?' sorusu karşımıza çıkmaktadır.

Bu sorunun cevabını başka bir örnekle incelediğimizde; Polonya Havayolları olan LOT'un sistemini de hackleyen bilgisayar korsanları, şirketin uçuş bilgilerini değiştirerek 10 uçağın kalkışını engelleyip, 12 uçağın da rötar yapmasına sebep olmuştur[18]. Yani bir uçak sisteminin kontrol mekanizması bir bilgisayar tarafından ele geçirilebilmektedir. Oysaki uçaklar çatışmalar ve gözlemler sırasında güvenilir araçlar olarak görülmektedir. Bu örnekler uçakların artık sanıldığı kadar güvenilir bir araç

[12]Uydularla Konum Belirleme Sistemlerinin Siber Güvenliği (Bölüm-2), 2018, https://www.airlinehaber.com/uydularla-konum-belirleme-sistemlerinin-siber-guvenligi-bolum-2/ adresinden 02.01.2019 tarihinde ulaşıldı.
[13]Havacılıkta Siber Güvenlik-I, http://www.cezerisga.com/makale/havacilikta-siber-guvenlik-–i adresinden 07.01.2019 tarihinde ulaşıldı.
[14]F35 YENİDEN Türkiye'nin gündeminde! Peki F35 nedir? F35 özellikleri neler?, 2018, https://www.haberturk.com/f-35-yeniden-turkiye-nin-gundeminde-peki-f-35-nedir-f-35-ozellikleri-neler-iste-detaylar-2101693/6 adresinden 03.01.2019 tarihinde ulaşıldı.
[15]Dünyanın beklediği proje F35 Siber Saldırı, 2016, https://www.memurlar.net/haber/484952/dunyanin-bekledigi-proje-f35-e-siber-saldiri.html adresinden 05.01.2019 tarihinde ulaşıldı.
[16]Boeing üretim tesisi Wannacry fidye saldırısına uğradı, 2018, http://www.milliyet.com.tr/boeing-uretim-tesisi-wannacry-teknoloji-haber-2636806/ adresinden 05.01.2019 tarihinde ulaşıldı.
[17]Havacılıkta siber saldırı tehlikesi, 2015, http://www.airporthaber.com/havacilik-haberleri/havacilikta-siber-saldiri-tehlikesi.html adresinden 05.01.2019 tarihinde ulaşıldı.
[18]Hackerlar 22 uçağın sistemine saldırı düzenlendi, 2015, https://www.sabah.com.tr/dunya/2015/06/22/hackerlar-22-ucagin-sistemine-saldiri-duzenledi adresinden 06.01.2019 tarihinde ulaşıldı.

olmaktan çıktığının kanıtlar niteliktedir. Bilgisayar sistemleri, teknolojinin gelişmesi ile beraber uçakların işlevlerini elinde tutarak egemen güç haline gelmeye başlamıştır.

Bir başka bahsedilmesi gereken olay ise tüm dünyanın dengesini değiştiren 11 Eylül saldırılarıdır. Bu saldırılarda 4 uçak El-Kaide örgütüne ait 19 kişi tarafından kaçırılmıştır[19]. Peki dünyanın en güçlü hava kuvvetlerine ait olan bu dört uçaktan hiçbirini neden fark edilip durdurulamamıştır? Çünkü saldırılar sadece uçaklara yapılmamış, aynı zamanda radar sistemlerine de bir siber saldırı gerçekleştirilmiştir. Bu örnekten yola çıkarak şu iddia ortaya atılabilir: Bir operasyon sırasında görevlendirilen bir savaş uçağı bilgisayar sistemi sayesinde ele geçirilip görevinin tersi yönünde hareket ettirilebilir ya da düşürülebilir ve radar sistemlerinin ele geçirilmesiyle beraber savaş uçağına yapılan bu siber saldırıdan bir süre haber alınamayabilir. Bu da operasyonun seyrini değiştirebilecek kadar tehlikeli sonuçlara neden olabilir.

İlginç olaylardan biriside, 2013'te gerçekleşen Samy Kamkar isimli bir hackerın kendi insansız hava aracını uçurarak gökteki başka insansız hava araçlarını bulması ve onları hackleyerek kontrollerini eline geçirmiş olmasıdır[20]. Bu tarz kritik siber saldırıların uçakları ele geçirmesi hem uçaklara olan güveni sorgulamakta hem de egemenliğin değişen sınırlarını ortaya koymaktadır.

Daha önce çalışmada bahsedilen İran tarafından ele geçirilen ABD'nin Lockheed Martin RQ-170 Sentinel isimli İnsansız Hava Aracına gelirsek; 4 Aralık 2011 yılında gerçekleşen bu olayda, bu insansız hava aracı Keşmar kenti yakınlarında İran kuvvetleri tarafından ele geçirilmiştir. İran hükümeti yaptığı açıklamada, insansız hava aracının Siber Birlik Birimi tarafından uçağı komuta ederek iniş yaptırdığını ifade etmiştir. Benzer bir örnek NASA'ya ait olan insansız hava aracına gerçekleştirilmiştir. Bilgisayar korsanları tarafından gerçekleştirilen bu siber saldırı da NASA'ya ait olan ve değerinin 220 milyon dolar olduğu ifade edilen Global Hawk isimli insansız hava aracı Pasifik Okyanusu'na düşürülmek istenmiş ve bu çerçevede hizmet sağlayıcısına siber saldırı yapılmıştır. İnsansız hava aracı bu olaydan son anda kurtarılmıştır[21]. Bu örnekler insansız hava araçlarının güvenlik sisteminde açıklar olduğunu ortaya koymaktadır.

Bu örnekler çoğaltılabilir, ancak verilen örnek olaylarda da görüldüğü gibi günümüz teknolojisinde artık illegal yollarla teknolojik araçların olduğu birçok sistem ele geçirilebilir duruma gelmiştir. Ekonomik hacim olarak oldukça yüksek fiyatlara sahip olan havacılık sisteminin siber saldırılara ve tehditlere çok boyutlu olarak açık olması dikkate alınması gereken bir konudur. Çünkü havacılık sektörü rutin operasyonların dışında kritik operasyonlar da giderek elektronik sisteme bağlanmaktadır. Elektronik sistem içinde saldırının çok hızlı cereyan etmesi bu sistem üzerinden gerçekleşecek olan bir siber saldırının önceden tesit edilip önlem alınmasını zorlaştırmaktadır. İnternetin bu denli gelişmesi bilgisayar sistemlerinin uçakları ele geçirecek seviyeye ulaşarak egemenliği ele almasını sağlamıştır.

3. Yürütülen Çalışmalar

Peki bu tehlikenin farkında olanlar yok mudur? Elbette ki vardır ve bu çerçevede çalışmalar kısmı de olsa yürütülmeye başlamıştır. Geçtiğimiz yıl ABD'de düzenlenen *Black Hat Konferasında Satcom Terminals (Uydu Terminalleri)* konulu bir sunum yapan güvenlik uzmanı **Ruben Santamarta** küresel uydu tabanlı iletişim ağına erişim sağlayan yer istasyonlarının yeterli güvenlik seviyesine sahip olmadığını ifade etmiştir. Santamarta hazırladığı raporda uçaklarda uydu bağlantıları ile ilgili iletişim sağlayan donanımları test ettiklerini ve çoğunda güvenlik açıkları bulduklarını açıklamıştır. Uçaklardaki güvenlik açıklarının kapatılarak her türlü korumanın sağlanması gerektiğini belirtmiştir[22].

Ayrıca Uluslararası Sivil Havacılık Organizasyonu (ICAO), 2016 yılında meclisinin 39. Oturumunda sivil havacılık için siber güvenlik konusuna değinmiştir. Havacılık sisteminin kritik altyapısının, iletişim ve bilgi sistemlerinin, verilerinin korunması konusunda koordinel bir çağrışım

[19]Mehmet Can Kömürcü, 11 Eylül saldırısı nedir? 11 Eylül saldırısını kim yaptı, 2018, http://www.milliyet.com.tr/11-eylul-saldirisi-nedir--11-eylul-saldirisini-kim-yapti--molatik-9280/ adresinden 03.01.2019 tarihinde ulaşıldı.

[20]Uydularla Konum Belirleme Sistemlerinin Siber Güvenliği (Bölüm-2), 2018, https://www.airlinehaber.com/uydularla-konum-belirleme-sistemlerinin-siber-guvenligi-bolum-2/ adresinden 02.01.2019 tarihinde erişildi.

[21]Hasan Karakuş; Sivil Havacılık Sektörü ve Siber Güvenlik; İnsansız Hava Araçları Örneği, Erciyes Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi, Yayınlanmamış Lisans Tezi, Erciyes, 2017, s.49-50.

[22]Yahya Reşat Dınler, Uçakları hackerlemek mümkün mü, 2015, https://h4cktimes.com/arastirma-ve-analiz/ucaklari-hacklemek-mumkun-mu.html adresinden 08.01.2019 tarihinde erişildi.

yapmıştır. Havacılıkda siber güvenliğin sağlanması için her türlü iş birliğinin yapılması gerektiğini ifade etmiştir[23].

2017 yılında Habertürkde çıkan bir haber de Alman ordusunun alarm verdiğini ve yayınladıkları raporda hackerların düşük maliyetle elde edebilecekleri ekipmanlar ile savaş uçaklarının kontrolünü ele geçirebileceklerini hatta bu savaş uçaklarını düşürebileceklerini ifade ettiklerini yazmıştır. Tümgeneral Ansgar Rieks tarafından yazılan bu rapor Almanya Savunma Bakanlığını da harekete geçirmiştir[24]. Almanya Savunma Bakanlığı bu çerçevede politikalar ve çalışmalar yürütmeye başlamıştır. Görüldüğü üzere artık internetin bulunduğu veya internetin bağlı olduğu bütün sistemler tehlike altına girmiştir.

Bugünlerde Berlin merkezli bir veri güvenliği firmasında çalışan Hugo Teso, aynı zamanda bir pilot olduğu ve hatta geçerli bir ehliyeti olduğu için, özellikle havacılık sektöründe teknoloji güvenliğiyle ilgili söyledikleri ciddiye alınması gereken biri olarak görülmektedir. Teso'nun çalışmaları göstermektedir ki bir uçağı uzak mesafeden kaçırmak için bilgisayara bile ihtiyaç yoktur. Teso'nun geliştirdiği PlaneSploit isimli bir uygulamaya sahip herhangi bir akıllı telefon bu işlem için yeterli olabilmektedir. Teorik olarak, siber-teröristler bu tip bir uygulamayı veya benzer bir teknolojiyi kullanarak uçakların sistemlerine girebilir ve uçağın düşmesine sebebiyet verebilirler. Teso bu konuların dikkate alınarak çeşitli önlemlerin alınması gerektiğini vurgulamıştır[25].

2018 yılındaki 26. DEFCON konferansında da ise insansız hava araçlarıyla yönelik ilgili siber saldırı ve siber güvenlik unsurlarını ele almaya odaklı çalışmalar yapılmıştır. Yapılan konferans da insansız hava araçlarına yapılan saldırılar dikkate alınarak insansız hava araçlarındaki açıklar ortaya konmaya çalışılmıştır. Ayrıca bu konferansda uçakların komuta kontrol sistemlerinin ele geçirilmesi üzerine de odaklanılmıştır[26].

Savunma Teknolojileri Mühendisliği A.Ş.'nin (STM) Teknolojik Düşünce Merkezi tarafından Aralık 2018'de yayınlanan Siber Tehdit Durumu raporu da bu alanda yapılan çalışmalar arasına girmektedir. Bu raporda 2019 yılında siber saldırıların artacağı öngörülmüştür. Raporda havacılık sektörünün hızla geliştiğini ve enerji gibi birçok kritik alan ile doğrudan bağlantılı olmasının riskleri arttırdığı ifade edilmiştir. Siber tehdide dikkat çeken bu raporda birçok kuruluşun siber tehditler ile tek başına başa çıkamayacağı bu yüzden de siber güvenlik faaliyetlerinin Siber Füzyon Merkezlerine dahil edilmesi gerektiğini savunmuştur[27].

ABD 'kıyamet günü uçağı' olarak tanımladığı E-4B Nightwatch isimli uçağı havalandırmıştır. Bu uçak birçok avantaja sahip olmakla beraber uçak olası bir savaş sırasında ABD Başkanı ve komuta kademesine ev sahipliği yapacaktır. Bir hafta havada kalabilme özelliğine sahip olan uçağın bir diğer özelliği ise siber saldırılara karşı oldukça dayanıklı olmasıdır[28]. İlk kez bir uçağın elektromanyetik saldırılara karşı savunma kapasitesine sahip olması bu konuda önlemlerin alınmaya başladığını göstermektedir.

Siber saldırıların ve tehditlerin atması buna ek olarak ülkelerin ve uluslararası kuruluşların siber alanında kendilerini geliştirme çabaları Türkiye'nin de siber alana yoğunlaşmasını ve siber güvenlik adına çalışmalar yapmasına sebep olmuştur. Türkiye, siber güvenlik adına ilk belgesini 2009 yılında Ulusal Sanal Ortam Güvenlik Politikası olarak çıkarmıştır. Bu politikada siber güvenlik ile ilgili temel terimler, açıklar, tehditler, alınması gereken önlemler ve stratejilerden bahsedilmiştir. Daha sonra yeni bir düzenleme ile Siber Güvenli Kurulu'nun sorumluluğu Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredilmiştir. Fakat Türkiye'de siber tehditleri genel çerçevede ele almış hava sistemlerine ayrıca yoğunlaşma göstermemiştir[29].

---

[23] Mahir Yüksel, Siber Güvenlik Perspektifinden Havacılık Endüstrisi, http://www.netcom.com.tr/2019/01/30/siber-guvenlik-perspektifinden-havacilik-endustrisi/ adresinden 27.03.2019 tarihinde erişildi.

[24] Alman ordusu alarmda: Hackerlar savaş uçağı düşürebilir, 2017, https://www.haberturk.com/dunya/haber/1562361-alman-ordusu-alarmda-hackerlar-savas-ucagi-dusurebilir adresinden 08.01.2019 tarihinde erişildi.

[25] Der Spıegel, Hackerlar uçak düşüre bilir mi? 2015, https://businessht.bloomberght.com/teknoloji/haber/1082852-hackerlar-ucak-dusurebilir-mi adresinden 08.01.2019 tarihinde erişildi.

[26] Uydularla Konum Belirleme Sistemlerinin Siber Güvenliği (Bölüm-2), 2019, https://www.airlinehaber.com/uydularla-konum-belirleme-sistemlerinin-siber-guvenligi-bolum-2/ adresinden 02.01.2019 tarihinde erişildi.

[27] Uçak Eğlence Sistemi Üzerinden, Uçağın Motorlarına Siber Saldırı Düzenlenebilir, 2019, http://www.milscint.com/tr/ucak-eglence-sistemi-uzerinden-ucagin-motorlarina-siber-saldiri-duzenlenebilir/ adresinden 27.03.2019 tarihinde erişindi.

[28] Kiyamet günü uçağı havalandı, 2018, https://www.ntv.com.tr/galeri/teknoloji/kiyamet-gunu-ucagi-havalandi-iste-e-4bnightwatchunozellikleri,CN3No8CcXkqI7rHNkwaBsg/Tk5Pf-Ik2k21aevYP2yUQA adresinden 08.01.2019 tarihinde erişildi.

[29] Sait Yılmaz ve Olay Salcan, *Siber Uzayda Güvenlik ve Türkiye*, İstanbul, 2008.

Fark edildiği üzere uçak sistemlerine siber saldırı örnekleri var olmasına rağmen uluslararası arena da hala bu konular yeteri kadar detaylı olarak ele alınmamakta ve önlemler için yeteri kadar çalışılmamaktadır. Bunun sebeplerinden birisi de siber saldırıların halen tam olarak bir savaş uçağını operasyon sırasında ele geçirmemesinden kaynaklanmaktadır. Ancak elde edilen veriler ve örnekler bu olasılığın çok da uzak bir zamanda gerçekleşmeyeceğini göstermektedir. Teknolojinin gelişmesiyle beraber siber tehdit araçlarının ve türlerinin artması beklenmektedir. Dolayısıyla bu artışlar ile beraber havacılık sektöründeki siber saldırıların da artması beklenmektedir.

SONUÇ

Uçaklar tarih boyunca savaşlar ve çatışmalarda önemli başarılar elde etmiştir. İkinci Dünya Savaşı'nda, savaşın kaderini bile değiştirmiştir. Halen daha uçaklar savaş, çatışma ve operasyonlarda kritik görevler yaparak ait olduğu ülkeye avantaj sağlamaktadır. Aynı zamanda havalimanlarının ve uçakların ülkelerin dünyaya açılan merkezleri konumuna sahip olmaları önemini bir kez daha ortaya koymaktadır. Atatürk'ün de son derece önem verdiği hava sistemi, siber dünyanın getirdiği tehlikeler ve tehditler karşısında önemini kaybetmektedir. Ülkeler de bu tehlikelere ve tehditlere karşı kısmen önlemler alıp, siber güç kapasitelerini ve güçlerini az da olsa arttırmaya çalışmaktadırlar. Aynı zamanda bilgi ve iletişim teknolojilerinin hala çok hızlı bir şekilde geliştiği göz önüne alındığında, ülkelerin siber güvenliğe yönelik eğilimlerinin daha da artacağı beklenmektedir. Ancak bu önlemler ne kadar yeterli olacaktır? Tam güvenli bir sistemin söz konusu olamadığı siber dünyada olabildiğince güvenli tabirini kullanmak daha isabetli olacaktır.

Ortaya atılan bir diğer teorisi ise siber saldırılar için alınacak olan önlemlerin yetersiz olacağı ve zamanla savaşların bilgisayar sistemleri tarafından gerçekleşen siber savaşlara döneceği düşüncesidir. Bu teori gerçekleşirse savaş uçakları önemlerini oldukça kaybedecek ve savaş sistemleri şekil değiştirecektir.

Çalışmada verilen örneklere bakıldığında uçak kontrol mekanizmasının siber saldırı sayesinde bir bilgisayarın eline geçtiğini görmekteyiz. Uçağın bir noktasından bilgi sistemine giriş yapacak olan bir virüs kısa sürede diğer tüm ağları ve sunucuları ele geçirerek kontrolü ele alabilir. Bu saldırıların radar sistemlerini de ele geçirmesi ölümcül sonuçlara neden olabilir. Bu sonuç da uçakların eskisi kadar egemenliği elinde tutmadığını ve onun yerine egemenliğin bilgisayar sistemlerine doğru kaydığını göstermektedir.

Çalışmada da bahsedildiği gibi henüz savaş uçaklarına operasyon sırasında direk bir siber saldırı gerçekleşmemiştir. Ancak bugün uçaklara karşı gerçekleştirilen saldırı örneklerinin ilerleyen konjonktürde savaş uçaklarını da ele alması gerçekleşecek hayali bir beklenti değildir.

Sonuç olarak, gelişen teknoloji ve yeni donanımlar karşısında sistemlerde açık ve zafiyetler her geçen gün artmaktadır. Artık siber saldırı atmosfer dışından, uydular aracılığıyla da yapılabilir hale gelmiştir. Yeterli güvenlik önlemleri alınmadıkça zamanın ne getireceğini tahmin etmek pek de zor olmamaktadır. Uluslararası arenada gerekli çalışmaların yapılmadığı ve uçaklara yapılan siber saldırılar ile ilgili hem iç hukuk da hem de uluslararası hukuk daki düzenlemelerin yetersiz olduğu göz önüne alındığında hava sistemlerine yapılacak olan siber saldırıların daha da artacağı sonucu ortaya çıkmaktadır.

Hava sistemlerinin güvenliği için hava trafik kontrol sistemlerinin, uçak sistemlerinin, uçak altyapı ve bilgi sistemlerinin olabildiğince siber saldırılara karşı geliştirilmesi gerekmektedir. Uluslararası hukuk çerçevesinde de bu yönde çalışmalar yapılmalı ve caydırıcı yaptırımlar uygulanmalıdır. Siber güvenlik, milli güvenlik bakış açısı ile ele alınarak farkındalık yaratılmalı ve gerekli önlemler alınmalıdır. İnsansız hava araçlarında yerli üretim yazılım ve donanımların kullanılması da yapılması gereken çalışmalar arasında sıralandırılabilir. Özellikle hava sistemlerinde kullanılan her türlü donanım, program ve servis sağlayıcıları düzenli olarak kontrol edilmesi gerekmektedir. Aksi taktirde hava sistemlerine saldırılar artacak ve bu da hava kuvvetlerinin önemini azaltacaktır.

KAYNAKÇA

Airlinehaber (2018). Uydularla Konum Belirleme Sistemlerinin Siber Güvenliği (Bölüm-2). https://www.airlinehaber.com/uydularla-konum-belirleme-sistemlerinin-siber-guvenligi-bolum-2/ adresinden erişildi.

Airporthaber. Havacılıkta siber saldırı tehlikesi,. http://www.airporthaber.com/havacilik-haberleri/havacilikta-siber-saldiri-tehlikesi.html adresinden erişildi.

Airporttürk. Uçak Nasıl İcat Edildi. http://www.airportturk.net/ucak-nasil-icat-edildi.html/ adresinden erişildi.

Cezerisga. Havacılıkta Siber Güvenlik- I. http://www.cezerisga.com/makale/havacilikta-siber-guvenlik---i adresinden erişildi.

Dervişoğlu, T. F. (2014). İstikbalini Göklerde Arayan Ülke Ve Türk Havacılık Sahasında Alman Menfaatleri Işığında Bir Ortaklık, *Cumhuriyet International Journal of Education-CIJE*, 3: 68-82.

Dınler, Y. R. (2015). Uçakları hackerlemek mümkün mü. https://h4cktimes.com/arastirma-ve-analiz/ucaklari-hacklemek-mumkun-mu.html adresinden erişildi.

Duman, Ç. (2018). *Jeopolitik Teoriler*. İstanbul.

Erenli, M. http://www.atam.gov.tr/dergi/sayi-04/ataturk-ve-havacilik/ adresinden erişildi.

Güntay, V. (2014). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler, *Güvenlik Stratejileri* , 27: 84-85.

Habertürk (2017). Alman ordusu alarmda: Hackerlar savaş uçağı düşürebilir. https://www.haberturk.com/dunya/haber/1562361-alman-ordusu-alarmda-hackerlar-savas-ucagi-dusurebilir adresinden erişildi.

Habertürk (2018). F35 YENİDEN Türkiye'nin gündeminde! Peki F35 nedir? F35 özellikleri neler. https://www.haberturk.com/f-35-yeniden-turkiye-nin-gundeminde-peki-f-35-nedir-f-35-ozellikleri-neler-iste-detaylar-2101693/6 adresinden erişildi.

Karakuş, H. (2017). Sivil Havacılık Sektörü ve Siber Güvenlik; İnsansız Hava Araçları Örneği, Yayınlanmamış Lisans Tezi, Erciyes: Erciyes Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi.

Memurlar.net (2016). Dünyanın beklediği proje F35 Siber Saldırı. https://www.memurlar.net/haber/484952/dunyanin-bekledigi-proje-f35-e-siber-saldiri.html adresinden erişildi.

Merkurbilet (2015). Uçağın İcadı ve Tarihsel Gelişimi. http://merkurbilet.com/blog/ucagin-icadi/ adresinden erişildi.

Milliyet (2018). Boeing üretim tesisi Wannacry fidye saldırısına uğradı. http://www.milliyet.com.tr/boeing-uretim-tesisi-wannacry-teknoloji-haber-2636806/ adresinden erişildi.

Milliyet. 11 Eylül saldırısı nedir? 11 Eylül saldırısını kim yaptı. http://www.milliyet.com.tr/ 11-eylul-saldirisi-nedir--11-eylul-saldirisini-kim-yapti--molatik-9280/ adresinden erişildi.

Milscrint (2019). Uçak Eğlence Sistemi Üzerinden, Uçağın Motoruna Siber Saldırı Düzenlenebilir. http://www.milscint.com/tr/ucak-eglence-sistemi-uzerinden-ucagin-motorlarina-siber-saldiri-duzenlenebilir/ adresinden erişildi.

NTV (2018). Kiyamet günü uçağı havalandı. https://www.ntv.com.tr/galeri/teknoloji/ kiyamet-gunu-ucagi-havalandi-iste-e4bnightwatchunozellikleri,CN3No8CcXkqI7rHNkwaBsg/AXK4c2dnB064mHLRXbLyRw adresinden erişildi.

İşcan, İ. H. (2004). Uluslararası İlişkilerde Klasik Jeopolitik Teoriler ve Çağdaş Yansımaları, *Uluslararası İlişkiler Akademik Dergi,* 1(2): 50.

Ponemon Institute, (2015) Cost of Cyber Crime Study: Global, Ponemon Institute Research Report, Michigan, s. 11.

Sabah (2015). Hackerlar 22 uçağın sistemine saldırı düzenlendi. https://www.sabah.com.tr/dunya/2015/06/22/hackerlar-22-ucagin-sistemine-saldiri-duzenledi adresinden erişildi.

Spıegel, D. (2015). Hackerlar uçak düşüre bilir mi. https://businessht.bloomberght.com/teknoloji/haber/1082852-hackerlar-ucak-dusurebilir-mi adresinden erişildi.

Türk Dil Kurumu (1960). http://www.tdk.gov.tr/index.php?option=com_bts&view=bts&kategori1=veritbn&kelimesec=309540 adresinden erişildi.

Wikizeroo. Fly-by-wire. http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWeub3JnL3dpa2kvRmx5LWJ5LXdpcmU adresinden erişildi.

Yılmaz, S. ve Salcan, O. (2008). *Siber Uzayda Güvenlik ve Türkiye,* İstanbul: Milenyum Yayınları.

Yüksel, M. Siber Güvenlik Perspektifinden Havacılık Endüstrisi. http://www.netcom.com.tr/2019/01/30/siber-guvenlik-perspektifinden-havacilik-endustrisi/ adresinden erişildi.