T.C.

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER VE GÜVENLİK ANABİLİM DALI

ULUSLARARASI İLİŞKİLER BAĞLAMINDA SİBER GÜVENLİĞİN İNSANSIZ HAVA ARACI (İHA) VE SİLAHLI İNSANSIZ HAVA ARAÇLARI (SİHA) ÜZERİNDEN DEĞERLENDİRİLMESİ

Yüksek Lisans Tezi

Çağrı GÜRBOĞA

Çorum- 2023

ULUSLARARASI İLİŞKİLER BAĞLAMINDA SİBER GÜVENLİĞİN İNSANSIZ HAVA ARACI (İHA) VE SİLAHLI İNSANSIZ HAVA ARAÇLARI (SİHA) ÜZERİNDEN DEĞERLENDİRİLMESİ

Çağrı GÜRBOĞA

Lisansüstü Eğitim Enstitüsü

Uluslararası İlişkiler ve Güvenlik Anabilim Dalı

Anabilim Dalı

Yüksek Lisans Tezi

TEZ DANIŞMANI

Dr. Öğr. Üyesi Mustafa COŞAR

Çorum 2023

KABUL VE ONAY SAYFASI

Çağrı Gürboğa tarafından hazırlanan "Uluslararası İlişkiler Bağlamında Siber Güvenliğin İnsansız Hava Aracı (İHA) ve Silahlı İnsansız Hava Araçları Üzerinden Değerlendirilmesi" adlı tez çalışması …/…/…… tarihinde aşağıdaki jüri üyeleri tarafından oy birliği/oy çokluğu ile Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Uluslararası İlişkiler ve Güvenlik Anabilim Dalında Yüksek Lisans/Doktora tezi olarak kabul edilmiştir.

Doç.Dr. Emre ÇITAK ……

Dr. Öğr. Üyesi Ebru GENÇALP ……

Dr. Öğr. Üyesi Mustafa COŞAR ……

Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun …/…/…… tarih ve …….. sayılı kararı ile ……'ın…… Anabilim Dalında Yüksek Lisans/Doktora derecesi alması onanmıştır.

Prof. Dr. Muhammed Asıf YOLDAŞ

Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını beyan ederim.

Çağrı GÜRBOĞA

ULUSLARARASI İLİŞKİLER BAĞLAMINDA SİBER GÜVENLİĞİN İNSANSIZ HAVA ARACI (İHA) VE SİLAHLI İNSANSIZ HAVA ARAÇLARI (SİHA) ÜZERİNDEN DEĞERLEDİRİLMESİ

Çağrı GÜRBOĞA

ORCID: 0000-00002-3890-9493

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Yüksek Lisans Tezi

Mayıs 2023

ÖZET

Uluslararası ilişkilerde var olan güç mücadelesi, 21 yy. ile fiziksel sınırları aşarak siber boyuta taşınmıştır. Siber uzayda bu alanlardan biridir. Fiziksel bir sınırın olmadığı küresel bir alandır. Siber alanda amaçlar doğrultusunda farklı aktörler bulunmaktadır. Aktörler tek başlarına bile siber alanda kendilerine yer edinebilirken, devlet ve devlet dışı aktörler tarafından da kullanılmaktadır. Kişi, kurum ve kuruluşlar gibi birçok aktör bulunmaktadır. Bu alanda aktör fazlalığının çok olması güvensizlik ortamını arttırmış ve etki alanını genişletmiştir. Devletler bu yüzden ulusal güvenliğin sağlanması konusunda ciddi önlemler almalıdır. Siber alan ile oluşan evrensel tehdit algısı artık devlet sınırlarının ötesindedir. Bu tehditi devletler ancak iş birliği yaparak çözebilir. Çünkü, uluslararası ilişkilerde tek bir güç olabileceği fikri gerçekliğe aykırıdır.

Bilişim sistemlerinin gelişmesiyle birlikte siber alan aktif kullanılmaya başlanmıştır. Aktif kullanılmasından dolayı siber alanda devletler güvenliklerini sağlamak için kendini tehdit unsurlarına karşı güçlendirmişlerdir. Devletler güvenlikleri için kendi yerli ağ bağlantılarını güvence altına almış, siber alan konusunda uzmanlaşmış kişiler veya kurumları ile iş birliği içerisinde olmuştur. Tehdit unsurlarının teknolojinin gelişmesiyle zaman içinde farklılaşmış ve artışlar olmuştur. Bu tehdit unsurların farklılaşmasına karşı yenilikleri ve teknolojiyi yakından takip eden devletler diğer devletlere karşı yarış içerisinde olmayı başarabilmişlerdir. Özellikle; Amerika Birleşik Devletleri (ABD), Kanada, İsrail, İran, Çin, Japonya, Birleşik Krallık, Rusya, Hindistan gibi ülkelerde bu alanda çalışmalar yapmaktadırlar. Bu siber saldırılara karşı Kuzey Atlantik Antlaşması Teşkilatı (NATO), Avrupa Birliği (AB), Birleşmiş Milletler (BM), Avrupa Konseyi gibi kuruluşlarda siber alan ve tehditler konusunda gelişme içerisindedirler.

Uluslararası ilişkilerde devletlerin barış algısını etkileyen siber saldırlar, güvenlik açısından istenmeyen ve dönüşü olmayan sorunlar yaratmaktadır. Çünkü devletler siber alanda kendilerine güç katarken, teknolojide yeniliği benimsemeyen, kendilerini siber alanda geliştirmeyen devletler siyasi ve askeri alanda güç kaybedilmesine neden olacaktır. İnsansız hava araçları (İHA) ve silahlı insansız hava araçları (SİHA) gibi teknolojilerin önemi dijitalleşme ile birlikte devletler için artmıştır. Burada kullanılan teknolojiler ile düşman birliklerin izlenebilmesi, anlık müdahale gibi süreçlerin yapılabilmesi, günümüz savaş sistemlerin eskiye göre artık daha otonom olduğunun göstergesidir.

İHA ve SİHA teknolojileri ise bu alanda son zamanların en dikkat çekici teknolojik gelişmeleri arasındadır. Bu gelişmeler sayesinde siber alanda yaşanılacak herhangi bir durumda İHA ve SİHA gibi araçlara sahip devletler, saldırının türüne göre bu araçların kullanılmasını sağlayabileceklerdir.

Bu tez çalışmasında, uluslararası ilişkiler bağlamında siber alan, siber güvenlik ve tehdit unsurlarının kavramsal anlatımlarının yanı sıra yeni nesil bilişim teknolojilerden, İHA ve SİHA' nın devletler için anlam ve önemini anlatılmaya çalışılmıştır. Bu gibi yeni nesil savunma sistemlerinin uluslararası alandaki dönüşümüne ve gelecekteki katkısına değinilmiştir.

Anahtar Kavramlar: Siber uzay, Siber tehdit, Siber güvenlik, İHA, SİHA

Bilim Kodu: 114111

EVALUATION OF CYBER SECURITY IN THE CONTEXT OF INTERNATIONAL RELATIONS THROUGH UNMANNED AERIAL VEHICLE (UAV) AND ARMED UNMANNED AERIAL VEHICLES (A-UAV)

Çağrı GÜRBOĞA

ORCID: 0000-0002-3890-9493

HITIT UNIVERSITY

GRADUATE SCHOOL

Master of Science Thesis

May 2023

ABSTRACT

The struggle for power in international relations has moved beyond physical boundaries to the cyber dimension with the 21st century. Cyberspace is one of these areas. It is a global space where there is no physical boundary. There are different actors in cyberspace for purposes. While actors can have a place in cyberspace even alone, they are also used by state and non-state actors. There are many actors such as people, institutions and organizations. The fact that there is a surplus of actors in this area has increased the atmosphere of insecurity and expanded its sphere of influence. Therefore, states should take serious measures to ensure national security. The universal threat perception created by the cyber space is now beyond the borders of the state. States can only solve this threat by collaborating. Because the idea that there can be only one power in international relations is unrealistic.

With the development of information systems, cyber space has started to be used actively. Due to its active use, states have strengthened themselves against threats to ensure their security in cyberspace. States have secured their own domestic network connections for their security, and have cooperated with people or institutions specialized in cyberspace. Threat elements have differentiated and increased over time with the development of technology. Against the differentiation of these threat elements, states that closely follow innovations and technology have been able to compete against other states. Especially;

Countries such as the United States of America (USA), Canada, Israel, Iran, China, Japan, the United Kingdom, Russia, and India are working in this field. Against these cyber attacks, organizations such as the North Atlantic Treaty Organization (NATO), the European Union (EU), the United Nations (UN), the Council of Europe are also developing cyberspace and threats

Cyber attacks, which affect the peace perception of states in international relations, create unwanted and irreversible problems in terms of security.Because while states add strength to themselves in the cyber field, states that do not adopt innovations in technology and do not develop themselves in the cyber field will cause a loss of power in political and military fields.The importance of technologies such as unmanned aerial vehicles (UAV) and armed unmanned aerial vehicles (A-UAV) has increased with digitalization.With the technologies used here, the ability to monitor enemy units and make instant interventions is an indication that today's war systems are more autonomous than in the past.

UAV and A-UAV technologies are among the most remarkable technological developments in this field of recent times. Thanks to these developments, states with tools such as UAV and A-UAV will be able to ensure that these tools are used according to the type of attack in case of any negativity in the cyber space.

In this thesis, besides the conceptual explanations of cyber space, cyber security and threat elements in the context of international relations, the meaning and importance of UAV and A-UAV, one of the new generation information technologies, for states are tried to be explained. The transformation and future contribution of new generation defense systems such as these in the international arena has been mentioned.

Key Terms: Cyber space, Cyber threat, Cyber security, UAV, A-UAV

Science Code:114111

TEŞEKKÜR

Yüksek lisans tez çalışmalarım süresi boyunca değerli yardım ve bilgileriyle bana yol gösteren saygıdeğer tez danışmanım Dr. Öğr. Üyesi Mustafa COŞAR'a ve yüksek lisans boyunca eğitim hayatımda önemli yer tutan hocalarıma teşekkürlerimi sunarım. Tez savunmama katılarak yapıcı eleştirileri ile tezin son halini almasını sağlayan değerli hocalarım Doç. Dr. Emre ÇITAK ve Dr. Öğr. Üyesi Ebru GENÇALP'e teşekkür ederim. Yüksek lisans yaptığım süre zarfında yorulduğum anlarda beni motive ve desteğini hiç esirgemeyen hayat arkadaşım Melike'ye destekleri için teşekkür ederim. Bütün eğitim hayatım boyunca hedeflerime ulaşma noktasında desteklerini iletmiş olan kız kardeşim Cansu GÜRBOĞA'ya, erkek kardeşim Ömer Can GÜRBOĞA'ya, sevgili annem Altun GÜRBOĞA'ya ve babam Mithat GÜRBOĞA'ya emekleri için çok teşekkür ederim.

Çağrı GÜRBOĞA

İÇİNDEKİLER

Sayfa

2.BÖLÜM

İNSANSIZ HAVA ARAÇLARININ TARİHSEL SÜRECİ

3. BÖLÜM

YENİ DÜZENDE ÇATIŞMA BİÇİMLERİNDE İHA VE SİHA

Sayfa

TABLOLAR DİZİNİ

Tablo **Sayfa**

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

RESİMLER DİZİNİ

Resim **Sayfa**

KISALTMALAR

Kısaltmalar

ABD	Amerika Birleşik Devletleri
AB	Avrupa Birliği
ARPA	İleri Araştırma Projeleri Ajansı
BM	Birleşmiş Milletler
BMGK	Birleşmiş Milletler Güvenlik Konseyi
CIA	Merkezi İstihbarat Teşkilatı
FLIR	Termal Kızılötesi
GPS	Küresel Konumlama Sistemi
İHA	İnsansız Hava Aracı
INS	Ataletsel (Inertial) Navigasyon Sistemi
MAM	Akıllı Mikro Mühimmat
NATO	Kuzey Atlantik Antlaşması Teşkilatı
NIR	Yakın Kızılötesi
RF	Rusya Federasyonu
SAR	Sentetik Aralıklı Radar
SİHA	Silahlı İnsansız Hava Aracı
UNIDIR	Silahsızlanma Araştırmaları Enstitüsü
VANET	Araçlar Arası İletişim
WLAN	Kablosuz Ağ
WSN	Kablosuz Sensör Ağı

GİRİŞ

İnsanlık tarihi kadar eski olan güç kavramı birçok kez yorumlanmış ve bilimsel çalışmaların temelini oluşturmuştur. Uluslararası ilişkiler açısından güce dair birçok sorgulamalar ve tartışmalar yapılmıştır. Birçok çalışmanın olmasına rağmen güç için ortak bir tanım yapılamamıştır. Yapılan çalışmalarda ortak bir tanımın yapılaması çalışmaların çeşitliliğini arttırmıştır.

21. Yüzyıl ile uluslararası ilişkilerde güç kavramının değişmeye başladığı bir dönemdir. Bilim ve teknoloji alanında yaşanılan gelişmeler uluslararası ilişkiler açısından güç ve güvenlik anlayışına yeni bir bakış açısı getirmiştir. Bu gelişmeler ile birlikte uluslararası ilişkilerde devletler kendilerine yer edinmeye ve rekabet alanı oluşturmaya çalışmışlardır.

Bilgisayar ve internet kullanımın hızlı bir şekilde artması ile siber alan kavramı daha sık kullanılmaya başlandı. Özellikle son zamanlarda siber uzay, beraberinde siber güvenlik, siber tehdit, siber istihbarat gibi birçok farklı alanların açılmasına neden olmuştur. İnternet ve ağ sitelerinin gelişmesiyle devletler bu alanlarda birbirleriyle daha sık iletişim kurmaya başladılar. Bu iletişim durumu beraberinde birçok risk ve tehdit durumun oluşmasını neden oldu.

Birçok imkan sağlayan siber uzaydan zaman geçtikçe fazlasıyla yararlanılmaya başlandı. Gündelik hayatta insanlar arasında etkileşimin artması, sosyal ağ bağlantılarının kullanılması, bankacılık ve finans işlemlerin halledilmesi, bilgiye daha çabuk ulaşılması gibi birçok faydası vardır. Devletler acısından siber alanın daha aktif kullanılmasıyla birlikte devletler arası ilişkiler, sağlık, ekonomi, eğitim gibi birçok süreçlerin yönetilmesi bilgilerin halka ulaştırılması, diplomatik faaliyetlerin daha hızlı bir şekilde gerçekleşmesi gibi birçok faydalar sağlanmıştır. Siber alan zaman içerisinde daha aktif kullanılması ile birlikte tehditlerin boyutu değişmiş ve ciddi sorunları oluşturmaya başlamıştır. Bu yüzden özellikle devlet, devlet dışı aktörler güvenilir ve yeni politikalar geliştirmeye başladılar. Ülke olarak Amerika Birleşik Devletleri, Çin, Türkiye gibi ülkeler ciddi çalışmalar yaparken NATO, AB ve BM, gibi uluslararası kurumlarda kendini bu alanda geliştirmeye çalışmaktadır. Siber alan artık yeni bir güç unsuru olarak görülmeye başlandı.

Çatışma alanlarında askeri zaiyatın daha az olması ve düşman unsurlarına daha çok zarar vermesiyle birlikte savaşlarda uzaktan kontrol edilebilen İHA ve SİHA'ya geçiş yapıldı. Artık gündelik hayatımız dahil birçok askeri, sivil ve ticari olaylarda İHA ve SİHA kullanılmaktadır. Diğer askeri hava araçlarından ise bazı noktalarda ayrılmaktadır. İHA ve SİHA içerisinde askeri bir personelin bulunmaması, uçuşunun otonom yapılar sayesinde uzaktan yapılabilmesiyle ve silahların çatışma türüne göre monte edilmesiyle diğer askeri hava uçaklarından ayrılmaktadır. Her ne kadar askeri personele ilk düzeyde ihtiyaç duyulmasa da acil ve beklenmedik durumlarda sorunun çözülebilmesi için uzaktan kontrol sayesinde bazı noktalarda çözüme ihtiyaç duyulmaktadır.

İHA ve SİHA'ya uzaktan müdahale edilmesi veya ele geçirilmesi gibi durumlarda pilotların bu durumlara hazırlıklı olması gerekir. Uzaktan savaşların kontrol edilebilme özelliği politikacılar açısından daha çok önemlidir. Çünkü halkın bu sürece sınırlı bir şekilde katılımı veya tepkisi diğer geleneksel savaş yöntemlerine göre daha az olmuştur. Birçok avantajda bulunmaktadır. Bunlar; teknolojik cihazların monte edilebilmesi ile farklı araç ve gereçle görevin zorluğuna göre donatılabilmesidir. Ayrıca alçaktan yapılan uçuşlarda fark edilmeden oranın detaylı görüntüsünün alabilmektedir. Yapılacak maliyetlerin diğer askeri teknolojilere göre daha ucuz olması İHA ve SİHA için önemli bir nokta oluşturmaktadır. Buna karşın İHA ve SİHA kullanımın zamanla artmasıyla birlikte birçok çatışma yaşanmıştır. Bu çatışmalarda sivil insanlara zarar gelmesi bu araçlara olan güvenin azalmasını ve eleştirelin yapılmasına neden olmuştur.

İHA teknolojisi özellikle 2000 senesinden sonra teknolojik dönüşümle kamuoyu tarafından daha bilinir olmuştur. İlk önce keşif ve gözetleme için askeri alanlarda kullanımına başlandı. Özellikle askeri alanda kullanılsa da sonrasında birçok alanda kullanılmaya başlandı. Düşman unsurlarına karşı taktik ve mekan üstünlüğünü elinde tutması vazgeçilmez olmasını sağlamıştır. Bu araçlara sonrasında askeri silah ve teçhizat yerleştirilmesi savaş alanında ciddi avantajlar sağlamıştır. Siber alanda aktif rol oynaması ile birlikte devletler için vazgeçilmez bir unsur haline gelmiştir. Yaygın kullanılmasında birçok neden vardır. Gözetleme ve keşif olaylarında düşman birliklerine karşı yakalanma olasılığı daha düşüktür. İnsana bağlı olarak bir yorgunluk ve sınırlı bir çalışma süreleri bulunmamaktadır.

Teknolojik olarak diğer hava araçlardan farklı olan İHA ve SİHA çatışma sırasında siber güvenlik unsuruna da dikkat etmesi gerekiyor. Çatışma ortamında bulunan alanın fotoğraflarını aynı anda komuta birimine sağlıklı bir şekilde aktarılması gerekiyor. Çünkü, komut ve kontrol merkezinde bulunun görevli kişiler ile İHA ve SİHA arasında veri transferi başarılı ve güvenli olmak zorundadır. Düşman unsurları tarafından ele geçirilecek bilgiler ciddi sıkıntılar oluşturabilir. Bu sırada veri transferinden bir bilginin ele geçirilmesi İHA ve SİHA'nın kaybedilmesi ve varolan koordinatların deşifre olmasına sebep olabilir. İstihbaratı önemli olan birçok bilgilerin de ele geçirilmesine sebep olabilir.

Çalışmanın birinci bölümünde; uluslararası ilişkilerde siber uzay kavramı incelenip, internetin tarihsel gelişiminden bahsedilecektir. Güvenlik kavramının detaylı incelenmesi sağlanıp siber alanda ki durumuna bakılmıştır. Uluslararası ilişkiler disiplinde harbin yeni yüzü olan siber savaş, siber suç gibi konulara değinilecektir. Bu konuların güvenlik açısından incelemeleri yapılıp uluslararası ilişkilerde güvenlik algısındaki değişmelerinin analizi edilecektir.

İkinci bölüme geldiğimizde ise, ilk kısımda bahsettiğimiz kavramlar çerçevesinde bağlantılı olacak şekilde İHA ve SİHA üzerinden analizler yapılacaktır. İHA ve SİHA'nın tarihsel gelişiminden bahsedildikten sonra tekniksel boyutlarla birlikte açıklanmaya çalışılmıştır. Çalışmanın ilk iki kısmında bahsettiğimiz kavramsal ve tekniksel analizler üzerinden incelemelerde bulunduk. Son bölümde ise bu incelemeler ışığında örnek olaylar ve günümüz

dünyasındaki bütünleşmesi incelendi. Bu sayede ulusal ilişkiler bakımından siber güvenliğin SİHA ve İHA üzerinden örnek olaylara sunarak bütünleşmesi sağlandı.

Araştırmanın amacı siber alanda yaşanan gelişmelerden bahsedilerek bu gelişmeler ışığında İHA ve SİHA'nın devletler için önemi uluslararası ilişkilerde güç kavramı gibi hususlarda detaylı incelemeler yapılacaktır. Dünyada 21. Yüzyıl ile farklılaşan güvenlik ortamında yeni tehdit unsurlarına karşı ulusal güvenliğin devletler açısından korunması noktasında İHA ve SİHA üzerinden ortaya koymaya çalışılmıştır.

Söz konusu bu çalışmanın uluslararası ilişkiler açısından önemi, askeri gücün her zaman devletler açısından ilk öncelik oluşturmasıdır. Sürekli değişen teknolojik süreçler uluslararası ilişkiler açısından güvenlik alanında yeni süreçlerin başlamasına neden olmuştur. Bu süreçlerde devletlere katkı sağlayacak olan İHA ve SİHA için incelemeler yapılıp değerlendirmeler sağlanmıştır. Uluslararası ilişkilerde bu durumun yeni olması ve türkçe kaynakların literatür bakımından az olmasından dolayı bu çalışma bazı boşlukların giderilmesine ve yeni çalışmaların oluşturulmasına katkı sağlayacağı düşünülmektedir.

Araştırmanın yönteminde ise özellikle uluslararası sistemde yer alan siber güvenlik, siber alan, siber tehdit, siber savaş, İHA ve SİHA gibi konulara önem veren makalelerden, tezlerden, resmi kurum ve kuruluşlardan, bilgiye önem veren rapor ve kaynaklardan yararlanılmıştır. Bunun dışında akademik ve bilimsel çalışmalarda kullanılabilecek, saygınlığı olan güvenliği ve doğruluğu ön planda olan kurumların internet sayfaları incelenip, buradaki verilerin görselleri kullanıp veri oluşturma sürecine dahil edilmiştir. Bu sayede betimleyici, örnekleyici ve özel bir çalışma olmuştur.

Planlı bir çalışma olan bu tez beş bölümden oluşmaktadır. Giriş ve sonuç bölümleri hariç 3 ana başlık bulunmaktadır. Bu yüzden literatür değerlendirmesi üç bölüm üzerine ele alınacaktır.

Birinci bölümün başlığı ''Siber Uzay Dahilinde Güvenliktir.'' İlk kısımda tanımlamalar dahil güvenlik ve siber alanın uluslararası ilişkilere bağlamında etkisi incelenecektir. Sonrasında İHA ve SİHA üzerinden tanımlamalar yapılacaktır. Son bölümde ise ilk iki bölümün günümüz uluslararası ilişkilerinde İHA ve SİHA'nın devletlerin güvenliklerine, askeri yapıları gibi birçok alandaki durumlarından bahsedilecektir. Bu hususta literatür incelendiğinde güvenlik alanında çalışmalar bulunmaktadır. Lakin uluslararası ilişkiler bakımından güvenlik konusunun İHA ve SİHA üzerinden empoze edilmesi, detaylı açıklanması ve farklı alanlarda inceleyerek literatürdeki boşluğu tamamlamaya çalışacaktır. Yeni yazılacak birçok araştırma içinde kaynak olabilecek bir eserdir.

1.BÖLÜM

SİBER UZAY DAHİLİNDE GÜVENLİK

1.1. Uluslararası İlişkiler Açısından Güvenlik Kavramı

Uluslararası İlişkilerin ana konularından birisi de güvenliktir. İçerisinde tehdit, rekabet, istihbarat ve fırsat gibi pek çok faktörü içeren güvenlik konusu günümüzde devletler tarafından daha çok önemsenmektedir. Çiçekçi (2012)'ye göre uluslararası ilişkiler disiplinleri arasında önemli görülen güvenlik kavramı hakkında akademik ve politik birçok yazı ve araştırma kaleme alınmaktadır.

1648 yılında Otuz Yıl Savaşı'nın sona ermesi ile Vestfalya Anlaşması imzalanmıştır. Bu antlaşma ile modern dünyanın temelleri atılmış, din savaşları sona ermiş ve uluslararası sistemde en güçlü aktör olarak devletler ortaya çıkmıştır. Zamanın getirmiş olduğu yenilikler sayesinde güvenlik algısındaki değişmeler devletler içinde inkar edilemez bir yere sahip olmuştur. Devletler tarafından ikili ilişkilerde karar verecek üst bir birimin olmaması ve güvenliklerini kendilerinin sağlayabilmeleri durumlarından dolayı başka alternatiflere gerek olmayacağı düşüncesindeydiler (Güntay, 2016, s. 7).

Karşı alternatifin olmadığı düzende ilk güvenlik çalışmaları, 2. Dünya Savaşı'nda ABD'li akademisyenler ile başlamıştır. Güvenlik konusunda yapılan ilk çalışmalar askeri alanda olmuştur. Bu alanda olmasının nedeni dönemin koşulları ve devletlerin uluslararası sistemde yaşamış oldukları gerilimlerden kaynaklanmaktadır (Çetinkaya, 2012, s. 247).

Güvenlik kavramının, farklı birçok anlamı olsa da en genel anlamı, karşı taraftan gelen tehditlerden korkmama, uzak kalma olarak tanımlanır (Karabulut, 2015, s. 7). Tarihsel olarak eski bir geçmişse sahip olan bu kavramın sosyolojik açıdan hala ortak bir tanımı yapılamamaktadır. Özellikle, uluslararası ilişkiler disiplininde birçok terimin alana dair fikir birliği sağlanarak tanımlanamaması paradigması buna örnek gösterilebilir (Özcan A. B., 2011, s. 447). Güvenlik kavramını biraz daha açmak gerekirse; devletlerin sahip olduğu sınırları askeri olarak koruması, herhangi bir saldırıya karşı savunması ve düşmanın geri püskürtülmesi olarak tanımlanabilir.

Geleneksel bakış açısına göre, güvenlik kavramı soğuk savaş ve sonrası dönemlerde farklılıklar göstermektedir (Payam, 2018, s. 16). Soğuk savaş dönemi, devleti merkez alan, askeri gücü de temel güç sayan ve ulusal çıkarları önemseyen bir dönem olarak özetlenebilir. Soğuk savaşta yaşanan süper güç olma mücadelesi batılı devletlerin ortak askeri ve güvenlik politikaları benimsemesine neden olurken diğer devletlerin güvenliğin farklı boyutları ile ilgilenmesine yol açmıştır. Soğuk savaşın bitmesi ile tüm dünyada hızlı bir küreselleşme sürecine geçilmiştir. Buna bir de kontrol edilemeyen nüfus artışı, sınırlar ve kıtalar arası göç, iklim değişiklikleri,

etnik ve ideolojik çatışmalar gibi olumsuz faktörler eklenince güvenliğin boyutları genişlemeye ve değişmeye başlamıştır. Bu sayede güvenlik kavramı artık siyasi, ekonomi, toplumsal ve çevresel birçok faktörle birlikte uluslararası konuları da dahil ederek kendisine yeni anlamalar yüklemiştir (İrdem & Bayansar, 2022, s. 144). Savaş sonrası dönemde ise devlet güvenliğini temele alan anlayıştan, bireysel ve toplum güvenliğine önem veren güvenlik anlayışına geçiş olmuştur (Bakan & Şahin, 2018, s. 45).

Zamansal ve dönemsel değişiklikler sonucunda kapsamı genişleyen güvenlik kavramının tanımını yapmak giderek zorlaşmaktadır. Özellikle son yıllarda 11 Eylül 2001 saldırısı ve Arap Baharı gibi olaylar tehdit, terör ve güvenlik kavramlarının sil baştan yazılmasına neden olmuştur. Diğer yandan internet, sosyal medya, mobil yaşam ve siber dünya gibi teknolojik gelişmeler kişilerin, toplumların devletlerin ve dünyanın bakış açısının tamamen değişmesine neden olmuştur.

1.2. Uluslararası İlişkiler Yeni Bir Boyut; Siber

Siber alan, 1982 yılında ilk kez bilim kurgu yazarı olan William Gibson tarafından kullanılmıştır. Siber kavramı burada ‘‘çağrışım yapan ve anlamsız’’ olarak tanımlamıştır. Daha sonra 1984 yılında yazmış olduğu Neuromancer adlı eserinde siber alanın karanlık yönüne değinmiş, kavranması mümkün olmayan karmaşık verilerin bulunduğu bir alan olarak tanımlamıştır (Ünal , 2015, s. 244).

Tanımlardan anlaşılacağı gibi siber alanın karmaşık yapısı ulusal ve uluslararası alanda tehditlerin algılama biçimlerine göre farklılık göstermektedir. Tehdit kavramı, her ne kadar gerçek unsurlara dayansa da farklı tahminlere ve algılara göre değişmektedir (Yorulmaz, 2014, s. 108). Güvenlik açıklarına yönelik yapılacak tehditler, öznel ve nesnel bir bakış acısıyla değerlendirilebilir. Nesnel bakış açısıyla bakıldığında gelecek tehditlerin büyüklüğü ile doğru bir orantı varken, öznel bakış açısıyla değerlendirildiğinde, sahip olunan değerlerin saldırıya uğrama korkusu vardır (Baharçiçek & İnan, 2013, s. 106).

Siber uzayın gelişmeye başlamasıyla siber güç, siber savaş ve siber güvenlik gibi birçok kavram ortaya çıkmıştır. Bu kavramlar sadece siber uzay üzerine çalışan akademisyenler dışında devlet ve devlet dışı aktörler tarafından da dikkatle takip edilmektedir. Bu derece önemli olmasında siber uzayın sahip olduğu tehdit unsurlarına karşı elde edilecek güvenlik çözümlerinin barış algısındaki değişimi ve dönüşümü etkili olmuştur.

Siber alanın sadece ulusal ve uluslararası güvenliği değil, ekonomik, teknolojik ve diğer pek çok alanı da etkileyebileceği ortaya çıkmıştır. Yeni güvenlik algısıyla beraber savunma kavramının da boyutları değişmeye başlamıştır (Bayraktar, 2014, s. 122). Siber alanın sahip olduğu asimetrik savaşa yatkınlık seviyesi, diğer savaş türlerine göre bir sınırının olmaması, yapılacak saldırılarının ani ve hızlı oluşu devletlerin güvenliklerini ve savunma sistemlerini bu yönde geliştirmelerine neden olmaktadır

Siber alanda silah olarak kullanılabilecek virüs ve zararlı yazılımlar devletlerin güvenliklerini tehlike altına sokmaktadır. Bu tehlikeler önceden tespit edilip gelecek herhangi bir saldırıya karşı önem oluşturup tamamen ortadan kaldırılması gerekir. Kritik altyapıların ve güvenliklerin sağlanması ancak bu alınacak önlemler ile mümkündür (Kotik, 2015, s. 9).

1.3. Uluslararası İlişkiler Açısından Tehdit

Her devlet güvenliğini tehdit edecek unsurlara karşı güvenlik önlemi oluşturmalı ve bunu stratejisi haline getirmelidir. Devletlerin bekasına ve varlıklarına gelebilecek saldırılar ulusal güvenliğin tehdit altında olduğunun bir göstergesidir (Kotik, 2015, s. 7).

Güvenlik algısı devletlerin yaşadıkları tehditlerin boyutlarına göre farklılıklar göstermektedir. Tehdit unsurları ile güvenlik arasında doğrudan bir ilişki vardır. Eğer bir kişi, devlet kendisini bulunduğu konumda güvende hissetmiyor ise bu durum tehdidin var olması ile alakalıdır. Olan tehdit kimi zaman gerçek olay ve olgular ile alakalı iken kimi zaman da tahmin düzeyinde kalmaktadır (Dedeoğlu, 2018, s. 22).

Devletlere yönelik tehditler kara, hava, deniz, denizaltı ve uzayda olmak üzere belli başlı alanlardan gelmektedir. Bu alanlara ek olarak bilgisayar ve ağları üzerinde bulunan yazılım, donanım, kullanıcılar ve uygulamalarının oluşturduğu siber alan ortaya çıkmıştır. Ayrıca siber alanın artan önemi ile sanal vatan gibi söylemler kullanılmaya başlanmıştır. Yakın zamanla birlikte artık fiziksel savaş alanlarının yerini sanal ortamlarda yapılan güvenlik açıkları üzerine giden siber alanlar almaya başlamıştır (Yener , 2013, s. 11).

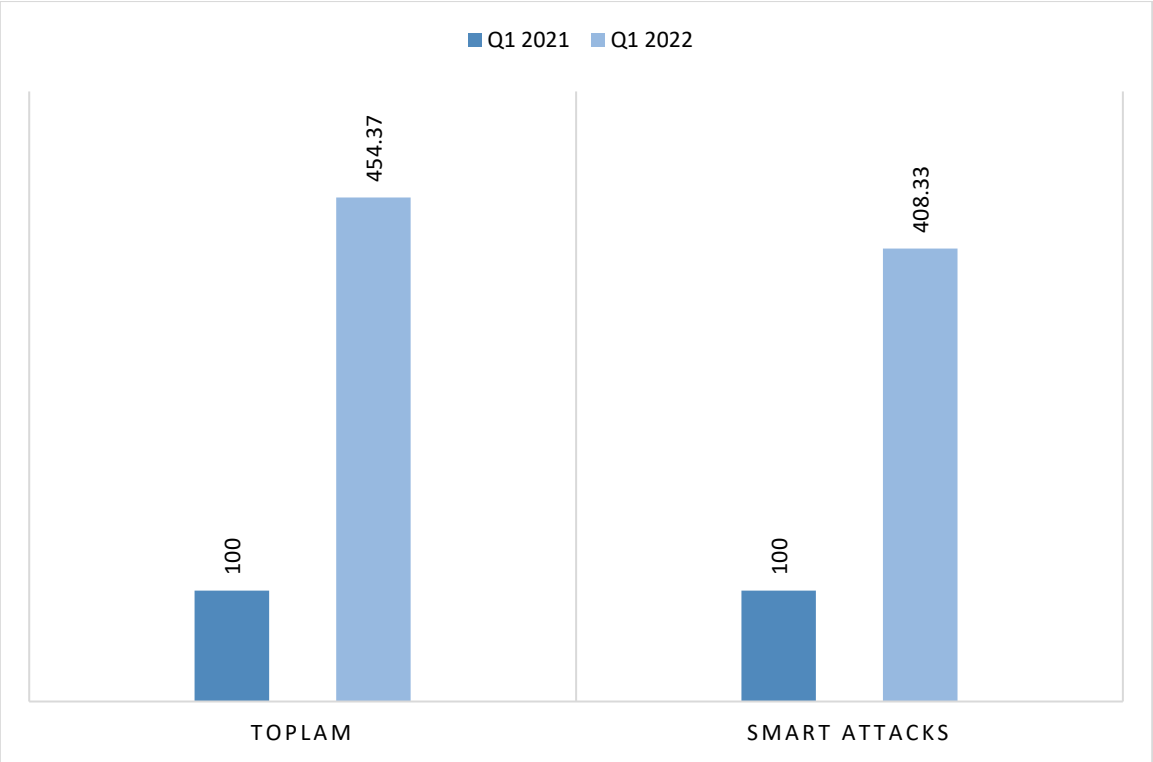
1.4. Siber Uzayın Güvenlik Açısından Genel Yapısı

İnternet ve bilişim sistemlerinin bu hızlı gelişimi güvenlik kavramına farklı bir boyut kazandırmış ve dünyanın güç dengelerinin değişmesine neden olmuştur. Devletler askeri alanın dışında siber uzayın getirmiş olduğu birçok alanda güvenlikleri sağlama ve yönetme konularında uzmanlaşmış ve güçlenmiştir. Siber uzaydan gelebilecek tehditlere karşı, sahip oldukları internet alt yapılarını ve güvenlik açıklarını kapatarak kendilerini koruma altına almaya çalışmışlardır. Verilerin sızdırılması veya açığa çıkması sadece devletleri değil güvenlik açısından birçok kesimi de ilgilendiren bir durum olmuştur. Kişisel olarak banka hesapları, özel fotoğrafları, videoları ele geçirilip ücret karşılığında geri satılabilir. Bu durumlar kişiler için psikolojik sorunlara yol açabildiği gibi maddi olarakta zor duruma düşmesine neden olabilir. İşletmeler açısından bakıldığında ise, bilgileri ele geçirilebilir ve mali açıdan değer kaybetmesine neden olabilir. (Barış , 2021, s. 9).

Yapılan saldırılar hem güvenlik hem de uluslararası toplum için önemli olup yakından ilgilenmesi gereken bir konudur. Amerika Birleşik Devletleri, Çin, İtalya, Rusya Federasyonu,

Birleşik Devletler gibi ülkeler siber alanda kendi güvenliklerini oluşturmaya çalışırken diğer yandan uluslararası hukuk bağlamından küresel önlemler almaya çalışmaktadırlar (Erdem & Özocak, 2019, s. 132).

Siber ortamda, birçok farklı sebepten dolayı saldırılar yapılmaktadır. Şekil 1.4'de görüldüğü gibi son 2 yılda yapılan servis dışı bırakma saldırıları olan (Distributed Denial of Servis-DDoS) bir grafiği aşağıda verilmiştir. Bu veriler 2022 yılının ilk çeyreğine aittir. Bu çeyrekte yapılan saldırılara bakıldığında gecen yıla göre 4,5 oranında bir artış olmuş, 2021 yılında ki saldırılara oranladığımızda ise %46 yani 1,5 katı kadar fazla siber saldırı olmuştur (Gutnıkov, Kupreev, & Yaroslav, 2022).

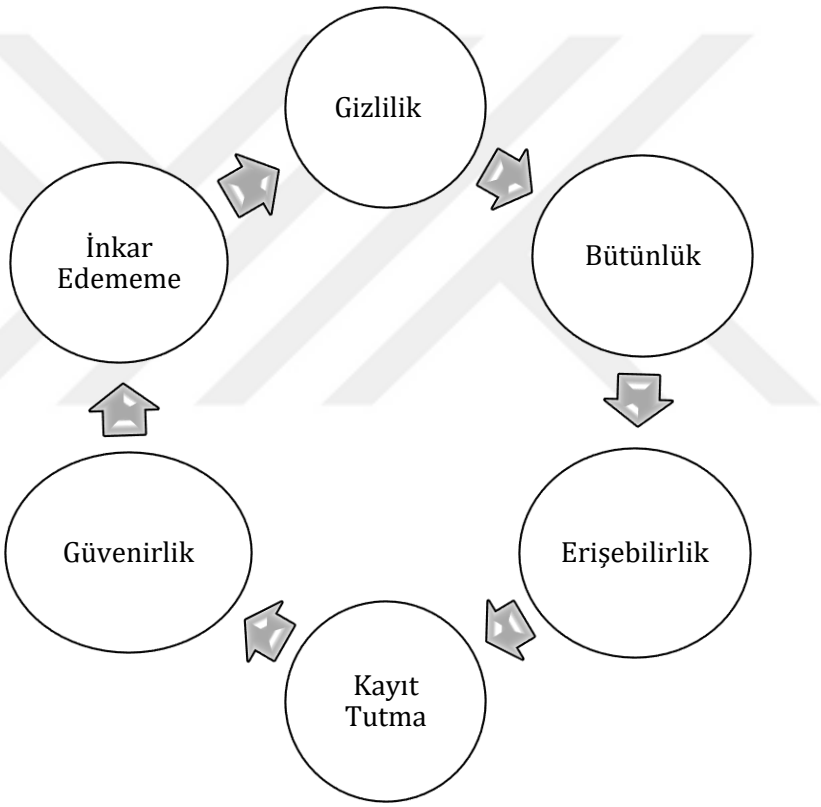


Şekil 1.4. 2021-2022 Yıllarının ilk Çeyreklerindeki DDoS Saldırılarının Karşılaştırılması (Gutnıkov, Kupreev, & Yaroslav, 2022)

Güvenlik tehdidi oluşturan siber saldırılar ciddi sıkıntılara sebep olur. Siber saldırılar sadece politik çıkarlar, kişisel verilerin çalınması, sistemlerin değiştirmesi gibi farklı amaçlar doğrultusunda kullanılabilir. Bundan dolayı güvenlik zafiyetine neden olur. Bireyler ve kurumlar bazından tehditler oluşturabilen siber olaylar, ulusal güvenliği tehdit etmeden, ekonomik çıkarlar elde etmek için diğer suçlar gibi işlenebilmektedir. Bu durum siber uzayın güvenlik açısından diğer tarafını oluşturmaktadır (Alioğlu, 2019, s. 7).

Kurum veya kuruluşların taraflarına gelecek saldırılara karşı elde etmiş olduğu verileri siber ortamda koruması gerekmektedir. Değişen teknolojik süreçler ile siber ortamda yapılan saldırlar sürekli değişmekte ve gelişmektedir. Saldırganlar sistemleri farklı yöntemler ile hizmet veremez hale getirmektedirler. Elde edilecek bilgiler ile maddi kazanç elde etmeyi düşünmektedirler. Kurumlar, sürekli gelişen ve farklılaşan siber uzayda, gelebilecek tehditlere karşı güvenliklerini sağlayamama durumunda itibarının zedelenmesi ve maddi kayıplar ile karşı karşıya kalmaktadırlar (Korkusuz, 2020, s. 17).

Siber uzayda güvenlik açısından ana argümanlarını gizlilik, bütünlük ve erişebilirlik şekilde sıralayabiliriz. Bu alanlardan biri veya birkaçından olabilecek bir yanlışlık ciddi sorunların yanında güvenlik zafiyetinin oluşmasına neden olacaktır



Şekil 1.5. Bilgi Güvenliği İlkeleri (Tekerek, 2008, s. 133)

Siber güvenliğin sağlanması kapsamında ilk önlem olarak, bilgi güvenliğinin temel unsuru olan gizlilik, bütünlük ve erişilebilirliğin sağlanması gerekir. Tablo 1.5'de görüldüğü gibi bilgi güvenliğinin temel unsuru olan bu unsurlara ek olarak güvenilirlik, doğruluk, inkar edememe, kayıt tutma, kimlik tespiti gibi unsurlarında eklenebilir. Gizlilik, elde bulunan veya elde edilen bilginin yetkisi olmayan kişiler tarafından ele geçirilmesi ve bunu korunması anlamına gelmektedir. Bütünlük, bilgilerin verilerin kişi veya kişiler tarafından değiştirilmemesi sürecidir. Erişebilirlik ise bilgiye ihtiyaç duyulması halinde, yetkisi olan kişilerin bu bilgilere

ulaşabilmesi ve istediği gibi kullanabilmesi anlamına gelmektedir (İşçi, Görmüş, Aydoğmuşoğlu, & Mekin Pesen, 2017).

1.5. İnternetin Tarihsel Gelişimi

İnternet, sivil teknoloji ile kullanılmaya başlandığı düşünülse de ilk askeri amaçlar doğrultusunda gelişmeye başlamıştır. Bu durum sadece bir noktada değil tüm ülkelerde böyle olmuştur (Yarman, 2011, s. 26). ABD ise bunun için savaş gibi olağan dışı durumlarda askerlerin kullanmış olduğu klasik haberleşme sisteminin kullanılamayacak şekilde tahrip edilmesi halinde tek bir bilgisayardan bağımsız çalışma düzenine sahip bilgisayar ağı kurabilmesi için çalışmalarına başlamıştır. Bu çalışmalar sonucunda İleri Araştırma Projeleri Ajansı (ARPA) kurulmasına karar verildi (Peker, 2013, s. 48).

İnternetin temeli Amerikan Savunma Bakanlığı desteği ve İleri Araştırma Projeleri Ajansı'nın ortak çalışmaları ile ARPANET projesi ile başlatılmıştır. Projenin ana amacı, gelebilecek herhangi bir askeri saldırı durumunda bilgi akışının devam ettirebilmesini sağlayacak bir ağ sistemi kurmaktı. 1971 yılına gelindiğinde bu projeye 24 araştırma ve kamu sitesinin birleştirilmesi ile ARPANET araştırmacıların kullanımına sunulmuştur.1989 yılında adının İNTERNET olması ile hızla gelişme göstererek günümüz halini almıştır (Yılmaz & Salcan, 2008, s. 35-37).

İnternet ilk olarak eğitim ve araştırma ağı olarak geliştirilmeye başlanmış ve bunun için araştırmacılar tarafından üzerinde çalıştıkları bir konu olmuştur. Yapılan çalışmaların dışına çıkan internet günümüz halini almış ve maksadının dışında kullanılmaya başlanılan bir alan olmuştur. Bugün ise askeri ve araştırmalar dışında özel sektör, kamu uluslararası şirketler gibi birçok alanda kullanılıp gelişme göstermeye devam etmektedir (Yılmaz & Salcan, 2008, s. 37).

21.Yüzyıl ile günümüzde artık bilgiler, veriler haberler, dokümanlar görülmemiş bir hızla yayılmakta ve uçtan uca iletilmektedir (Ünsal , 2010, s. 41). Ülkeler birbirlerinden ne kadar uzak olursa olsun dünya üzerinden bilgisayarların birbirleri ile olan ağ bağlantısı sayesinde iletişimi sağlayan internet 20. Yüzyılın son çeyreğinde ortaya çıkmış ve günümüze kadarda gelişimini devam ettirmiş en önemli teknolojik gelişmelerden biridir. İnternetin gelişmesi ile kıtalar arası mesafeler kısalmış, bilgiye ulaşma süreside azalmıştır (Özçoban, 2014, s. 49).

Özellikle internet ile gelişme gösteren en önemli yapı adını sıklıkla kullandığımız ağlardır. Günümüzdeki birçok teknolojik cihazın (telsiz, tablet, akıllı telefonlar gibi) ağ teknolojisinin gelişmesi internet ile olmuştur (Bıçakçı, 2013, s. 2). İnternet birçok yere şu an hızlıca bilgileri ulaştırma imkânı sağlamış bunu da bilgisayar ve iletişimin gelişmesi ile olmuştur. Birçok yerde bilgisayar kullanımın artması ile konumlar arası mesafeler önemsizleşmiş ve karşılıklı iletişimin sağlanması ile birçok işlem daha hızlı ve kolay bir şekilde çözüme kavuşturulmuştur (Çakmak & Altunok, 2009, s. 61).

1990 sonrası gelişmeye başlayan internet devletlerin, güvenliklerini ciddi anlamda tehdit etmeye başladı. Devlet sırları, kendilerine '' Hacker'' diyen kişiler tarafından ele geçirilmesi ile hem kendileri hem de diğer devletler sorunlar yaşamaya başladı. Bu kişiler sadece devletler ile değil büyük kentlerin iletişim ve altyapılarına sızarak büyük tehditler oluşturmaya başladılar (Özcan M. , 2014).

İnternet'in, 1990 yılından sonra gelişme göstermesi ile Soğuk savaş sürecinde avantaj sağlamıştır. Çünkü devletler arasındaki yüksek gerilimin düşmesi internet sayesinde olmuştur. Sadece devletler için değil insanlar arasındaki iletişimi sağlamasında da etkin bir rol oynamıştır İnternet için özellikle 1991 yılında Körfez Savaşının başlamasıyla detaylar canlı bir şekilde aktarılmıştır. Savaşın insanlar tarafından takip edilmesi gelecek yeni dönemin farklı olacağının göstermiştir (Bıçakçı, 2012, s. 207).

Son yüzyılın en büyük icatlarından olan internet, teknolojinin göstermiş olduğu yenilikler ile birlikte gelecek yıllarda kendisinden ve sağlamış olduğu faydalardan dolayı adını sıklıkla duymaya devam edeceğiz.

1.6. Siber Güvenliğin Uluslararası İlişkiler Açısından Genel Nitelikleri

İnsanların teknolojik gelişmeleri yakından takip etmesiyle birlikte interneti daha etkin bir şekilde kullanmışlardır. Bu sayede küreselleşme kavramı dünyamızı hızlı bir şekilde etkilemiştir. Teknolojinin gelişmesi ile her ne kadar insanlar bunu kullanmaya başlasa da uluslararası toplum için tehdit unsuru haline gelmiştir. Siber güvenlik bu bağlamda özellikle ulusal ve uluslararası alanda bireyleri, kurumları, devletleri geniş bir yelpazede incelememizi sağlayan bir konudur.

Bugüne bakıldığında, devletlerin güvenlik tehditlerine karşı teknolojik gelişmelerden habersiz olmaları düşünülemez. Siber güvenlikte devletlerin teknolojik olarak yetersiz kalması büyük tehlikeleri yaşayabileceği anlamını taşımaktadır. Uluslararası alanda devletler güvenliklerini, yaşanabilecekleri herhangi bir saldırı durumuna karşı planlamalı ve buna göre organize etmelidir (Darıcılı & Özdal, 2017, s. 139).

Siber güvenlik, ulusal ve uluslararası alanda bireyleri, şirketleri, örgütleri ve devletleri yakından ilgilendirmektedir. İnternetin ilk ortaya çıkması ile kapalı devre sistemlerinin birçok kurum ve kuruluşlara zarar veremeyeceği fikri hakimdi. Ancak bu sistemin sahip olduğu dezavantajlı olduğu bir durum vardı. Güven'inde (2021, s. 8) dediği gibi sisteme erişme yetkisi bulunan kişilerin siber güvenlik açısından sorun oluşturabileceğinin görülmesi ile kurum ve kuruluşlara zarar veremeyeceği görüşün doğru olmadığı ortaya çıkmıştır. Çünkü sistemi kontrol etme yetkisi bulunan kişilerin veriler üzerinden birçok kontrolü sağlama ve değiştirme olanağı bulunuyor.

Veriler, kullanıcılar tarafından bilgisayar üzerinden sağlanan veri akışı ağ üzerinden kaydedilmekte sonrasında bilgisayarlarda depolanmaktadır. Ağ sistemlerinin güvenli olması ve gelebilecek herhangi saldırıya karşı hazırlıklı olmak gerekir. Yapılacak herhangi bir saldırı güvenlik zafiyetleri oluşmasına neden olup bir yapının çökmesine sebep olabilir. Bu yüzden siber güvenlik uluslararası ilişkiler açısından hayati önem taşımaktadır (Başeskioğlu, 2021, s. 11).

Devletlerin siber güvenliklerini sağlamak için uluslararası ilişkiler açısından bu konuda güvenlik stratejileri oluşturması gerekmektedir. Çünkü burada alınmayacak bir önlem ekonomi dahil birçok alanın bozulmasına ve zarar görmesine neden olacaktır. Uluslararası alanda güvenlik önlemi almak artık bir zorunluluk haline gelmiştir. Ülkelerin rekabet edebilmelerinin ilk aşaması doğru ve gizli bilgiye sahip olmaktan geçmektedir. Bu nedenle elde edilecek bilgiler devletlere karşı avantaj oluşturarak kendi acılarında kullanabileceklerdir. Bu sayede devletler siber güvenlik alanında kendileri hem geliştirecek hem de gelecek dönem için kendilerini bu rekabet ortamına hazırlayabileceklerdir.

1.7. Güvenlikleştirme ve Siber Güvenlik

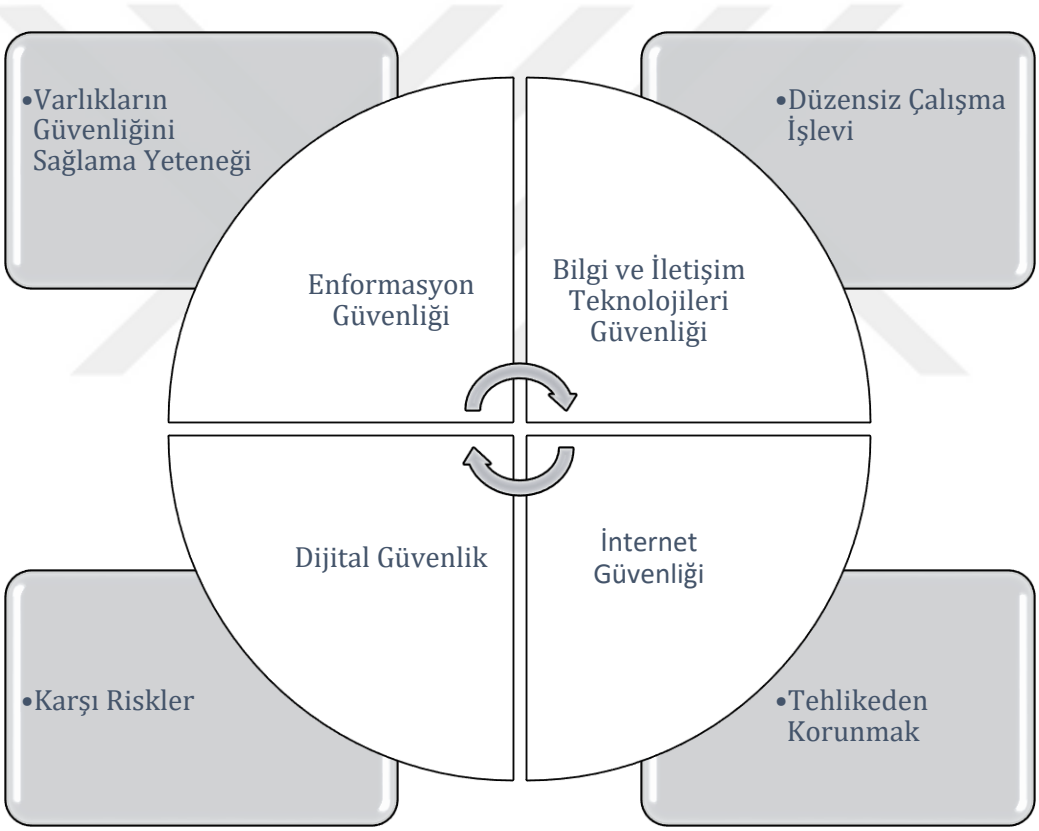
Devletler için siber alan artık vazgeçilmez bir muhabere alanı olmuştur. İnternetin ve teknolojinin karşılıklı etkileşiminin artması ile güvenlik alanında yeni bir parametre oluşmuştur. Karşılıklı yaşanan bu etkileşim siber güvenlik konusunda devletlere yeni sorunlar yaratmıştır. Yaşanan bu sorunların başında coğrafi sınırlar gelmektedir. Yeni güvenlik ortamında artık coğrafi sınırların bir önemi kalmamıştır. Özellikle siber güvenlik alanında verilecek bir açık ulusal ve uluslararası alanda zincirleme birçok sonucun doğmasına sebep olacaktır. Bazı devletler tarafından ise bu durum ikna ve cezalandırma aracı olarak kullanılmıştır. Ülkelerin güvenlikleri bu yüzden tehlike altına girmiştir.

Siber güvenlik, kişilerin dışında kurum ve kuruluşların özellikle siber ortamda kendi varlıklarını idame edebilmek için siber alanda var olan saldırılara veya risklere karşı korunaklı olmayı amaç edinen faaliyetler bütünüdür (Çiftçi, 2013, s. 8).Devletler güvenlik kaygılarını ortadan kaldırmak için silahlanmaya gidebilir ya da sorun yaşayan diğer devletler ile iş birliği yaparak alternatifler üretebilir. Bu tarz durumların oluşması özellikle bir silahlanma durumunun ortaya çıkması diğer devletler için güvenliğin azalıp, güvenlik ikileminin oluşması anlamına gelmektedir (Karabulut, 2015, s. 40).

Güvenlik endişeleri her gecen gün artarak dünya siyasetini daha çok etkilemeye başlamıştır. Güvenlik ikilemi, silahlanma gibi tanımlamalar ortaya çıkmıştır. Devletler ise bu sorunlar karşısında, güvenlik sorunlarını algılayıp, buna uygun tanımlamalar yapmıştır (Bilgiç, 2012, s. 339).

Özellikle devletlerin silahlanma konusunda ciddi bir yarış halinde olmasıyla birlikte siber güvenlik alanında kendilerini geliştirme çabaları, ekonomik olarak birçok alanda harcama yapılmasına neden olmuştur. Özellikle siber güvenlik alanında uluslararası ortamda caydırıcı görevler üstlenmek isteyen devletler, kendi sınırlarının dışına çıkıp çatışma haline girmişlerdir. Herhangi bir yasa koruyucu olmamasından dolayı sonuçları bir önceki güne göre daha kötü olmuştur (Güntay, 2016, s. 157-158).

Siber güvenlik, gelişen teknoloji ve değişen saldırı yöntemleri ile günden güne büyüyen bir sorun haline gelmiştir. Güvenli bir siber ortamın oluşturabilmesi için bazı faktörlerin önceden hazırlanması gerekir. Devletlerin özellikle siber alanda kendilerini geliştirmeye ihtiyaçları vardır. Tamamen güvenlikli bir siber ortamdan bahsetmek şu an için mümkün değildir. Aşağıdaki şekil 1.6'da siber güvenlik kapsamındaki güvenlik kavramlarının şeması verilmiştir.



Şekil 1.6. Siber Güvenlik Kapsamındaki Güvenlik Kavramları (Erdem T. , 2020, s. 156)

Günümüzde yaşanan birçok değişim ve gelişim ile özellikle tehdit algısındaki farklı dönüşümler ile siber güvenlik; dijital güvenlik, internet güvenliği, enformasyon güvenliği, bilgi ve iletişim teknolojileri güvenliği gibi birçok güvenlik türünden bahsedebiliriz. Her ne kadar güvenlik kavramı önceden tek bir kavram olsa da sonrada farklı kavramlara ve anlamlara ayrılmıştır.

Siber güvenliğe özellikle bilgi güvenliği açısından bakıldığında yazılım sistemleri içerisinde önemli bir alanı kapsamaktadır. Dijital ortamda ya da internet dahil birçok verilerin kullanımı, siber güvenlik için önem arz etmektedir. Çünkü siber güvenlik sadece bilgilerin ihlali konusunda değil kişinin kendi dahil birçok varlıkların güvenliğinden sorumludur. Burada olabilecek zararlara karşı korunmayı amaç edinmiştir (Bilen, 2021, s. 7)

1.7.1. Siber uzayla değişen güç, savaş ve barış algısı

Dünyanın bilgiye daha hızlı ulaşması ile siber uzay alanında farklılıklar oluşmaya başladı. Özellikle uluslararası alanda devletlerin siber uzay alanında kendi adlarından söz ettirme isteği, karışlıklı çatışmalara ve yeni bir alanın doğmasına sebep olmuştur. Bireylerin, kurumların, devletlerin kendilerini siber alanda geliştirme istekleri sahip oldukları bakış açısını değiştirdi.

Modern çağın başlamasıyla birlikte teknolojik alanlarda büyük değişimler yaşandı. Bu değişimler özellikle siber uzayda gerçekleşti. Eski savaş teknikleri artık kullanılmamaya başlandı. Geleneksel savaş türleri, insanlar için tehlikeli olmayan bir savaş türü haline geldi. Bu yüzden devletler yeni savaş türleri için farklı güvenlik stratejiler geliştirmek zorunda kaldılar.

Devletlerin uzun zamandır uyguladığı klasik güvenlik anlayışı artık yerini güvenlik anlayışına bırakmıştır. Bu anlayış değişikliğinin temel nedeni; siber uzayın diğer savaş türlerinin aksine kendi içerisinde sahip olduğu sınırsız bilgi teknolojisidir. Bunun yanında diğer savaş türlerine göre maliyeti daha düşüktür. Karşı tarafa verilen zarar diğer savaş türlerine göre daha fazladır (Tarhan, 2018, s. 52).

İlk başlarda diplomatik ve askeri konularda kullanılmaya başlanmıştır. İstihbarat için saklanmış ve gerekli tedbirlerin alınması için çalışmalar yapılmıştır. Bilgi teknolojilerin özellikle siber kavramının daha fazla gelişmeye başlamasıyla birlikte iletişim teknolojisi farklılaştı. Bu farklılıkta özellikle elde tutulan bilgi sayısallaşmasını ve istenildiği zaman kullanılması sağladı. Sayısallaşmasıyla birlikte bilgi güvenliği artık devletlerin ortak bir sorun haline geldi (Güngör , 2015, s. 5).

Yeni dönem ile birlikte uluslararası sistemde güvenlik anlayışı artık değişmeye başladı. Soğuk savaş bittikten sonra küreselleşmenin kendini daha çok hissettirmesi ile güvenlik anlayışı devletler üzerinden değişmeye başladı. Bu dönem ile birlikte artık askeri odaklı olmasından vazgeçilmiştir. Yeni süreç ile birlikte özellikle bilgi, insan, toplum güvenliği gibi yeni terimler kullanılmaya başlanmıştır (Güleç, 2021, s. 12).

Siber güvenlik sayesinde zaman ve mekân olarak etkileşimin artık ortadan kalkması ile yapılan saldırılar büyük etki bırakmıştır. Devletler bu etki karşısında, siber uzay için ciddi bütçeler ayırıp finansal kaynaklar bulma yoluna gitmişlerdir. Uluslararası ilişkilerde var olan güç dengesi artık değişmiştir. Eskiden bahsedilen coğrafi konum, stratejik düzey gibi var olan

askeri savaş kapasitelerinden bahsedilmemeye başlanmıştır. Devletler bunların dışında güvenliklerini korumak için değişen güç dengesini koruma amacına gitmiştir. Bu durumu ise ileri düzey teknolojik gelişmeler ışığında kendilerine bu alanda geliştirmeyi amaç edinmişlerdir. Tüm bunlar dönemin koşulları gereği olarak değerlendirildiğimizde, uluslararası ilişkilerde devletler için artık artan iş birliği düzeyi ile birlikte istihbarat olarak bilgi paylaşımının, yapılması en büyük ihtiyaçlardan biri olmuştur. Çünkü siber alanda oluşabilecek bir saldırı sonrası tüm dünyadaki ulusal refah düzeyi etkilenebilir ve barış unsuru ortadan kalkabilir (Idan, 2020, s. 82).

Siber alanda yer alan ve barış unsurunu etkileyecek en önemli konuların başında bilgi güvenliği konusu yer almaktadır. Artan nüfus ve bilgi teknolojilerin değişmesi ile sistemin güvenliği zorlaşmıştır. Kişiler, kurumlar, devletler için yapılacak en önemli adım ise sistemi tehdit edecek unsurları belirleyip buna göre tedbir almasıdır. Bilgiye sahip olan kişiler, kurumlar, devletler tarafından korunması gereken önemli bir husustur. Sürekli bir tehdit olgusu haline gelinebilir.

Devletler artık yeni güvenlik anlayışında kendilerini daha güvende hissedebilmeleri için siber uzayda yer alan teknolojik gelişmeler bağlamında kendilerini geliştirmelidir. Bu gelişmeyi yakalayamayan devletler ciddi güvenlik sorunları ile karşılaşabilir. Askeri alanda devletlerin geleneksel savaş stratejileri ve organizasyonlarından uzaklaşıp yeni dünya düzeninde yer almaya başlayan devletler, siber uzay alanında yeniden organize olup kendi güvenlik algısını buna göre yeniden inşa etmelidir (Çelik, 2018, s. 111).

1.7.2. Siber uzayın uluslararası ilişkilerde etki aracına dönüşmesi

Siber uzayda, devlet ve devlet dışı aktörler kendi kullanıcılarına ait güvenlik bilgilerine siber ortamda koruyabilmelidir. Bu ortam içerisinde siber uzayda değişen saldırı türlerine karşı güvenlik adına uluslararası ilişkilerde yeni politikalar üretilmeye başlanmış, sistem üzerinde dahil olan tüm aktörler ve bireyler bu alanda kendini geliştirmeye başlamıştır. Siber uzayın konuşulmaya başlandığı bu dönemde birçok etki aracı ortaya çıkmıştır. Özellikle siber müdahalelerin yapılabilmesi için siber alanda yer alan saldırı teknikleri ve yöntemleri geliştirilmeye özen gösterilmiştir.

Günümüzde siber uzay, devletlerin birçok kurum ve kuruluşunda önemli görevler üstlenmektedir. Bu görevlerin başında alt yapıların oluşturulması ve güvenliklerin sağlanması konusunda siber uzay önemli bir rol üstlenmiştir. Siber uzay ile birlikte güvenlik sistemlerin değişmesiyle, uluslararası ilişkilerde güç dengesi farklılık göstermiştir Askeri güç, devletler için sahip olunması gereken tek statüden çıkmıştır. Siber uzayın yenilikçi yapısını kendine görev edinmiş devletler, kendilerini bu alanda güçlendirmeye çalışmış askeri gücün alternatiflerini kullanmaya çalışmışlardır.

Siber uzayın diğer önemli bir yanı devletler arasındaki sınırların kaldırılmasıdır. Bu sadece devletlerin değil bireylerin de bilgilere erişmesini kolaylaştırmıştır. Bu kolaylık siber uzayda bir güvenlik açıklarına neden olmaktadır. Bu açıklar doğrultusunda siber uzayın uluslararası ilişkilerde önemi her geçen artmaktadır.

Siber uzayın kendi içerisinde birçok tehdit unsurları ile kuşatılmış olması güvenlik açısından yeni fikirlerin ortaya çıkmasına sebep olmuştur. Özellikle kendilerine siber uzayda gelebilecek herhangi bir tehdit unsuruna karşı internet alt yapılarını, ağ bağlantılarını korumaları gerekir. Çünkü devletler, siber uzay gibi bir alanda güçleri bazında yeni stratejiler geliştirerek, sosyal düzeni korumaya uluslararası barışın devam etmesi için elinden geleni yapmışlardır (Arslan, 2021, s. 20).

1.8. Siber Güvenlik ile İlgili Kavramlar

1.8.1. Siber alan

Uluslararası sistemde devletler kendilerini teknolojik olarak sürekli geliştirmektedirler. Bu gelişmeler beraberinde birçok değişimi getirmiştir. Özellikle internet alanında yaşanılan gelişmeler ile siber uzay yeni bir harp alanı olarak görülmeye başlanmıştır. Kara, deniz, hava ve uzaydan sonra siber alanda savaşlar içerisinde kendine yer edinmiş, harbin beşinci boyutu nitelendirilmesinde bulunulmuştur. Böylece uluslararası alanda yer alan aktörler gelebilecek tehditlere karşı artık daha kapsamlı düşünüp, etkin savunma planları uygulamak durumunda kalmışlardır.

Siber kelimesinin kökeni eski Yunan tarihine kadar dayanmaktadır. Yunancada ‘‘kübernetes’’ anlamına gelmektedir. Kelime kökeni olarak ise sibernettik kavramı esas alınmıştır. Sibernettik kavramının ilk olarak 1958 yılında Louis Couffignal tarafından kullanılmıştır. Louis bu dönemde özellikle canlılar ve makineler üzerine araştırmalar yapmıştır. Bu araştırmalarda canlılar ve makinelerin aralarındaki iletişimi incelemiştir (Emir, 2020, s. 5).Bilişim sistemlerin ağlar üzerinden birbirine bağlanıp sayısal verilerden algoritmalar oluşturarak bilgiler üretilmesi, siber alan sayesinde olmuştur. Siber alanın farklı birçok yan anlamı bulunmaktadır. Siber uzay, siber dünya bunlardan akla ilk gelendir. Uzay veya alan gibi yeni anlamlarının bulunmasında, siberin hem dünya üzerinden hem de uzaya yayılmış olmasından kaynaklıdır.

Siber uzay veya Siber alan kavramı Amerikalı yazarı William Gibson tarafından ilk kez 1982 yılında yazdığı kitapta kullanılmıştır. ABD Savunma Bakanlığı için siber uzay; İnternet ve bilgisayarların kontrol birimlerini içeren teknolojik birçok yeni alt yapı oluşturan ve bu alt yapılar sayesinde bilgilerin küresel alanda var olmasına denir. Diğer bir tanıma göre siber uzay; kişilerin veya devletlerin varlıklarının devamını idame ettirebilmesi için kritik altyapıların sunucular sayesinde kablolar ile iletişimin sağlandığı alan olarak nitelendirilmiştir. Her ne kadar siber alan kavramı soyut bir alanmış gibi gelse de siber alan bunun dışındandır. Harbin

beşinci boyutu görülen siber alan kendi içerisinde fiziksel bileşenlere sahiptir. Yüksek ve maliyetli fiber kablolardan meydana gelmektedir. Bu kablolar bir sunucuya bağlanmakta ve yönlendirilmekte kullanılmaktadır. Bu alt yapının bir toprak parçasında bulunarak bileşenler dahilinde ülkenin topraklarına nüfus ederek orada yer edinmektedir. Bunun dışında yazılım destekli telsizler, insansız hava araçları, silahlı insansız hava araçları enerji dağıtımları gibi yazılımsal ve üst teknolojik donanımlar siber alanın kendisini oluşturmaktadır (Özçoban, 2014, s. 51).

Siber alan kavramını dört ana başlık altında toplamak mümkündür. Birinci başlık; sistemlerin oluşmasını, devam etmesini yani sürekli olmasını sağlayan fiziksel birimlere denir. Bu birimler ilk olarak karadan geçen kabloları, haberleşme için uyduların bulunmasının yanında yönlendiricilerle iş birliği olmasına sebep olan fiziksel yapılara denir. Mantıksal yapılar ise siber uzayın ikinci yapısını oluşturmaktadır. Bunu yaparken; tarayıcılar, sistemler, güncellemeler gibi farklı alternatifler kullanılır. Diğer unsur ise bilgidir. Telefon üzerinden yapılan mesajlar, mailler, resimler, sosyal ağlar aracılığıyla yazılan metinler bilgileri oluşturur. Siber alanın en önemli yapısı ve tüm bu bileşenlerin karşılıklı etkileşimde bulunması sağlayan insan figürü vardır. Elde edilen bilgiyi kullanıp bunu fiziksel ve mantıksal yapılar ile taşıyan sonrasında ise kendi güvenliği için kullanıp saklayan en önemli unsurdur (Ulutaş, 2018, s. 87-88).

Siber alanda yapılan saldırılar diğer saldırılardan farklı olarak ışık hızında gerçekleşir. Geleneksel saldırılarda böyle bir durum yoktur. Yapılan saldırının hızlı bir şekilde gerçekleşmesi verilen etkinin de en az konvansiyonel silahlar kadar etki göstermektedir. Bu yüzden devletler kendileri modern toplum bağlamında yüksek teknoloji ile donatmaya özen göstermektedir. Siber alanda yapılan bir saldırının hangi sebeple yapıldığı veya kim tarafından yapıldığının bilinmemesi onun diğer yanını oluşturmaktadır. Geleneksel savaşlar ve siber savaşlar konusunda bu tarz farklılıklar oluşturmaktadır (Gürkaynak & İren, 2011, s. 265).

Tablo-1.8. Siber Alanın Özellikleri ve Riskleri (Kotik, 2015, s. 6)

Özellik	**Risk**
Kendine has yazı dilinin olması	Belirli kişilerce anlaşılacak kod, resim veya video ile verilerin aktarılması.
Hızlı olması	Kısa bir zaman diliminde kargaşa ortamının yaratılıp, örgütlenme faaliyetlerinin sağlanması.
Birçok aktörün bulunması	Devlet, kurumlar veya bireyler arasında çatışma durumunun olması. Geniş eylemlere uygun olma.

Evrensel Özelliğe sahip olması	İstihbarat konusunda oluşabilecek herhangi bir açıkta, Uluslararası gündemi değiştirecek devlet bilgilerin açığa çıkması.

Siber alan sayesinde yeni birçok kavram ortaya çıkmıştır. Siber suç, siber savaş, siber istihbarat gibi kavramlar, bunlardan bazılarıdır. Uluslararası sistemde devletler tarafından artık üstünde durulması gereken konuların başında gelmektedir. Bu tür kavramların olması siber alanda gelebilecek tehdit unsurlarına karşı devletleri zor durumda bırakabilir ve güvenlik zafiyetlerinin oluşmasına sebep olabilir.

1.8.2. Siber suç

1990 yılından sonra internet gelişmesiyle birlikte insanlar bu gelişimleri yakından takip etmiştir. Yaşanan bu gelişmeler insanlar tarafından benimsenmiş ve kullanılmaya başlanmıştır. İnternet için yaşanan bu hızlı değişim, batı dünyasına daha çok yansımıştır. İnternetin bu derece benimsenmesi ve hızlı yükselişi de bazı olumsuzlukları beraberinde getirmiştir.

Siber uzayın kendine has özelliğinden dolayı net bir tanım yapılamasa da birbirine yakın tanımlamalar yapılmıştır. Her ne kadar bu durum olumlu gibi görünse de siber alan kontrolün zor olduğu her daim birçok tehlikenin var olabileceği bir ortamdır. Siber suç ise, belirli kişiler tarafından yürütülen küresel ağlar sayesinde yasadışı işlemlerin bilgisayarlar üzerinden yapılarak suç unsuru oluşturmasına denir (Cengiz, 2021, s. 410).

Küreselleşmenin hem insanlar için hem de devletler için hız kazanmasıyla bazı değişimler oldu. Bu değişimler, özellikle güvenlik alanında yaşandı. Siber uzayda bilgiler baz alınarak yapılan saldırılarının artış göstermesi, siber suçlar ile güvenlik kavramlarını karşı karşıya getirmiştir. Bilgi teknolojilerinin hızlı dönüşümü sağladığı kolaylıklar ve imkanlar doğrultusunda, siber alana daha bağımlı hale gelmemize sebep olmuştur. Bu ortam içerisinde siber alanda suçların artarak kişilerin can ve mal güvenliğine zarar vermesinde dolayı güvenlik anlayışlarında değişiklikler yaşanmıştır (Şenol, 2016, s. 11).

İnternet ve bilgisayarlar üzerinden yapılan işlemlerin her gecen gün artış göstermesiyle birlikte siber alanda işlenen suçlarda farklılık göstermektedir. Elektronik ortamda ve ağ bağlantılarının olduğu bir sistemde yapılan işlemlerin hukuka uygun bir şekilde yapılmaması sonucunda siber suç türünü ortaya çıkarmıştır. Bu alanda yapılan her işlem siber suç kapsamında değerlendirilemeyeceği gibi belli başlı siber suç türleri bulunmaktadır. Diğer suç türlerine göre işlenen suçların, şekillerinin farklı olması siber suç kavramını ayrı kılmaktadır. Bu hususta Tablo-1.9'da siber suçlar konusunda örnekleri verilmiştir.

Tablo 1.9. Dijital Suç Türleri (Cengiz, 2021, s. 412)

SUÇ	**TANIMI**
Dolandırıcılık	Özel kazanç elde etmek için bilgisayarda yer alınan verilen değiştirilip satılması ve kötü amaçlı kullanımın sağlanması
Hırsızlık	Birçok kurumsal birimlerin müşterileri için yapabilecekleri çevrimiçi işlemleri sınırlı tutup e-hırsızlığı önlemeye çalışmak.
Lisanssız yazılım kullanımı	Orijinal yazılımlar dışında kopya yazılımlar kullanmak.
Siber terörizm	Sanal ortamlarda terör propagandası oluşturmak ve teşvik etmek.
Özel İş	Kişinin kazanç elde edebilmesi için var olan kuruluşun sahip olduğu olanakları izinsiz kullanması.
Kişisel bilgilerin kötü amaçlar için kullanılması	Bilgisayarda içerisinde uygun olmayan sitelerde gezinme ve elde edilen verilerin kötüye kullanılması.
Hackleme	Erişim yetkisi olmadığı bir sayfaya izinsiz giriş sağlamak ve bilgileri kullanmak.
Sabotaj	Ekipmanlara zararlı kasıt vererek bilgisayarlarda ki süreci uzatmak.
Pornografik Materyal Tanıtmak	İnternet sayfalarından pornografik İçeriklerin tanıtılması.
Casusluk	Kişilerin, çevrimiçi kişisel bilgisayarlara saldırarak gizli bilgilerin toplanması sağlamak.
Virüs	Karşı tarafın bilgisayarını bozmak amacıyla program dağıtmak veya yüklemek.
Çevrimiçi Hizmet Reddi	Karşı tarafın bilgisayarlarına zarar vermek için virüs veya e posta engellemeleri gibi tekniklerin kullanılmasıdır.

Siber suçların diğer geleneksel suçlardan farklı olarak ayrıldığı bazı noktalar vardır. Siber alanda yapılan saldırının sonuçları bir başka devletin sınırlarında görülebilir. Siber suçlarda verilen cezaların az olması ya da kanunlarda boşlukların fazla olması suçların bu alanda yapılmasını artırmaktadır. Siber alanda yapılan bir suçun kim tarafından yapıldığının bulunması çok zordur. Siber suçlarda alınan önlemler geleneksel savaş yöntemlerine göre daha yenilikçi olup hızlı bir şekilde gelişme göstermektedir. Teknolojinin gelişmesi ile siber suçlar

farklılık gösterdiği için buradaki suçlar artık farklılaşmaktadır. Diğer savaş türlerine göre siber alanda az bir birikim ile ciddi siber suçlar işlenebilmektedir. Bu alanda ki kişiler suç işlerken birlikte olsalar da sonrasında ayrılıp organize bir örgütlendirme gerçekleştiremiyorlar. Yapılan suçların tekli ve çoklu olması herhangi bir şey ifade etmemektedir. Çünkü herhangi bir sorumluluk bilinci bulunmamaktadır (Sandilaç, 2021, s. 51).

1.8.3. Siber savaş

Siber savaş kavramından önce savaş kavramına bakmamız gerekir. Savaş, uluslararası sistemde devletlerin birbirlerine karşı ilanda bulunarak silahlı çatışma yapmasına denir. Bu hususta siber savaş ise devletlerin siber uzayda veya siber alanda karşılıklı savaşma haline denir. Tanımlamalar konusunda eksiklikler olduğu gibi yapılan saldırıların hangilerinin siber savaş statüsünde değerlendirileceği konusunda ortak bir karar bulunmamaktadır. Bunun birçok nedeni bulunmaktadır. Bazı akademisyenler siber savaşa fazla önem verildiğini, olabilecek herhangi bir saldırının bir savaş olarak değerlendirilemeyeceğini vurgulamaktadır. Devletler tarafından yapılacak siber saldırının ise şiddetli bir karışıklık yaratma düşüncesinin yanında silahlı bir çatışmaya dönüşmeyeceği fikrindedirler. Lakin Gürcistan ve Estonya'ya karşı yapılan siber saldırılar bu alanın bize önemini göstermiştir. Siber saldırılardan sonra uluslararası sistem savaş hukuku üzerinden yoğunlaşmıştır. BM sözleşmesinin 51. Maddesi genel kaide olarak alınarak meşru müdafaa hakkı düşünülmüş ve birçok kişi tarafından savunulmuştur (Yayla, 2014, s. 183-184).

BM teknolojik gelişmelerden geri kalması aslında bunun bir başka sebebidir. Bilgi devriminden BM ileriye dönük siber alanda olan gelişmeleri yetersiz ele alıp potansiyel tehdit olarak görmemesi siber savaşların başka boyutunu oluşturmaktadır. Çünkü konvansiyonel savaşlarda silah, askeri teçhizat gibi savaş unsuru sayılacak kavramlar değerlendirmeye alınırken, siber alanda bir silah kavramının değerlendirilmesi tartışma sebebi olmuştur (Sandilaç, 2021, s. 58).

Eski Başkan George W. Bush döneminde siber alanda danışmanlık görevini Richard Clarke üstlenmişti. Clarke siber savaş için, ülkelerin bilgisayarlar veya ağlar üzerinden kesinti yapmak üzere gerçekleştirdikleri saldırı veya sızma faaliyetleri olarak açıklamıştır. Tanımlardan da anlaşılacağı üzerine iki noktaya dikkat edilmelidir. Bunlardan ilki, siber savaş devletler arasında olur. Diğer durum ise; Bir saldırının siber savaş olarak değerlendirebilmesi için karşı tarafa zarar verme veya bir kesinti oluşturma gayesi içerisinde yapılması gerekir (Çiftçi, 2013, s. 5).

Siber savaşın silahları üç kategoriye ayrılmıştır. Sentetik, semantik ve karışık saldırılar. Sentetik saldırıların genel amacı; karşı tarafın bilgisayar sistemine girip zararlı virüs yazılımları ile sistemin çalışmasını engellemeye çalışırlar. Semantik saldırı ise sentetik saldırıdan farklı olarak amaç, sistem yöneticisini veya kullanıcının elde ettiği verinin doğru

olup olmadığını hedef alır. Bu saldırılar özellikle devletin resmi kurum sitelerine veya ülkeler için hayati derece öneme sahip olan altyapı tesislerini hedef alarak ciddi zararlar vermeyi amaçlar. Son olarak karışık saldırılar ise hem semantik hem de sentetik saldırıların aynı anda yapılması ile oluşur (Yayla, 2014, s. 187-188).

Siber savaş diğer savaş türlerinden farklı olarak genel amacı para kazanmak için yapılır. Politik veya siyasi siber savaşlarda yapılmaktadır. Siber savaşlar terörizmden farklı olarak değerlendirilir. Bu politik düzende her ne kadar ülkeler siber savaş ve terör eylemlerini desteklese de amaçları bakımından farklılık içermektedir. Özellikle siber savaşlarda, terör saldırılarında farklı olarak sistematik ve sürekli saldırılar gerçekleştirilir. Siber savaşlar yapılırken temelinde devlet veya bir otorite tarafından yapılır. Terör saldırılarında ise bu durum daha çok bireyler ya da gruplar halinde kendisini göstermektedir. Bu yüzden kişisel olarak herhangi bir siber saldırı yapıldığında bu durum siber savaş statüsünde değerlendirmeye alınmamaktadır (Çakmak & Altunok, 2009, s. 44-45).

1.8.4. Siber istihbarat

Siber istihbarat kavramının tanımı konusunda siber dünyanın diğer konuların da olduğu gibi net bir tanım yapılamamaktadır. Bu başlık altında ilk olarak istihbarat kavramı üzerinden bilgilendirmeler yapılmıştır.

İnsanoğlu var olduğu andan itibaren merak ve korku hislerini yönlendirmek istemiştir. Gelecekte kendilerine ne tür tehlikelerin beklediği konusunda bilgi sahibi olmak için birtakım çalışmalar yapmıştır. Yapılan savaşlarda, karşı tarafın bir sonraki hamlesini öğrenme çabası istihbarat alanının doğmasına bunun bir disiplin olmasına neden olmuştur. İstihbarat konusunda ilk çalışmalar Sun Tzu tarafından yapıldığı düşünülmektedir. Sun Tzu devletlerin kendileri savaş alanında güvende hissedebilmeleri için yapılacak aldatmacalara karşı temkinli olmayı dile getirmiştir (Demir, 2001, s. 43-45).

İstihbarat kavramının farklı birçok tanımı bulunmaktadır. Yapılan tanımlamalarda dikkat çeken unsur, bilginin ön koşul olarak karşımıza çıkmasıdır. İstihbarat konusunda Bimfort geniş bir tanımlama yapmıştır. Bimfort'a göre istihbarat; Ülkenin güvenliği konusunda stratejiler oluştururken bunu dış politika bağlamında değerlendirip elde edilen bilgileri işleyerek, politika yapıcılar tarafından kendilerine yardımcı olmak için ifşa olmadan çalışma sağlanması sürecine denir (Yılmaz B. A., 2020, s. 73).

Teknolojinin gelişmesi ile geleneksel savaşlarda kullanılan istihbarat yöntemleri de farklılık göstermeye başlamıştır. Yeni dönem ile birlikte siber istihbaratta artık teknik, sinyal, iz istihbaratı gibi daha önemli konulara bırakmıştır. İnternetin hızlı gelişimi ile bilgiye ulaşma süresi kısalmıştır. Bilgisayarların bu süreçte daha aktif rol oynaması ile istihbarat için personel ihtiyacı azalmıştır. Bilgilerin toplanması, tasnif edilmesi gibi birçok süreçte bilgisayarların

önemi anlaşılmış ve siber istihbarat için vazgeçilmez olmuştur. Bilgilerin artması ve ulaşma süresinin azalması sadece bilgisayara olan yüksek bağımlılığın yanında internete duyulan ihtiyacı da artırmıştır. Devletler, gelebilecek siber saldırıları engellemek için yoğun caba harcar. Yapılan bu saldırılara karşı, yöneticilere bilgi verilip sürecin eksiksiz yürütülmesine ve gerekli tedbirlerin alınmasına siber istihbarat denir (Bayraktar, 2014, s. 130).

Siber istihbarat alanında devletler, kendi yöntemlerini oluşturma çabası içerisine girmişlerdir. Bilgi teknolojilerinin sürekli gelişme halinde olmasından dolayı yeni yöntemler gelişmekte ve kendilerine karşı savunma süreci uygulamaktadırlar. Geleneksel olarak bakıldığında istihbarat, konularına göre birçok ayrıma tabi olmaktadır. Siber istihbarat bulunduğu alanın genişliğinden dolayı yöntemlerine göre sınıflandırılmasıda yapılabilmektedir. Girgin bundan dolayı siber istihbaratın iki yönünü vurgulamıştır. Bunlardan birincisi, bilgisayarlar bilgi gönderim işlemlerini ağ bağlantıları sayesinde kolay ve hızlı bir şekilde sağlamaktadırlar. Diğer yönü ise bilgisayarlar ağ bağlantıları sayesinde bilgi gönderirken çeşitli virüs, zararlı yazılımlar sayesinde bilgiler ele geçirilebilir veya değiştirilebilir (Girgin, 2003, s. 383).

2.BÖLÜM

İNSANSIZ HAVA ARAÇLARININ TARİHSEL SÜRECİ

2.1. İnsansız Hava Araçlarının (İHA) Tarihi

Teknolojinin zaman geçtikçe gelişmesiyle birlikte kullanımı artmıştır. Bundan dolayı insan yaşamını etkilemeye başlamıştır. Özellikle hava araçlarında yaşanan gelişmeler ile havacılık sektörü gelişmeye başlamıştır. Teknolojide yaşanan bu gelişmeler askeri alanda kendini göstermeye başlamıştır. Özellikle yer araştırması, haberleşme, arama kurtarma, savunma sanayisi veya bir bölgede olan suçların gözetlenmesi gibi birçok alanda aktif kullanılmaya başlanmıştır. Aktif kullanılmasında birçok sebep vardır. Özellikle İHA'ların geniş bir alanı inceleyebilmesi, doğru ve net sonuçların alınabilmesi, zaman konusundan insanlara tasarruf sağlaması aktif kullanılmasında başlıca sebepler olmuştur.

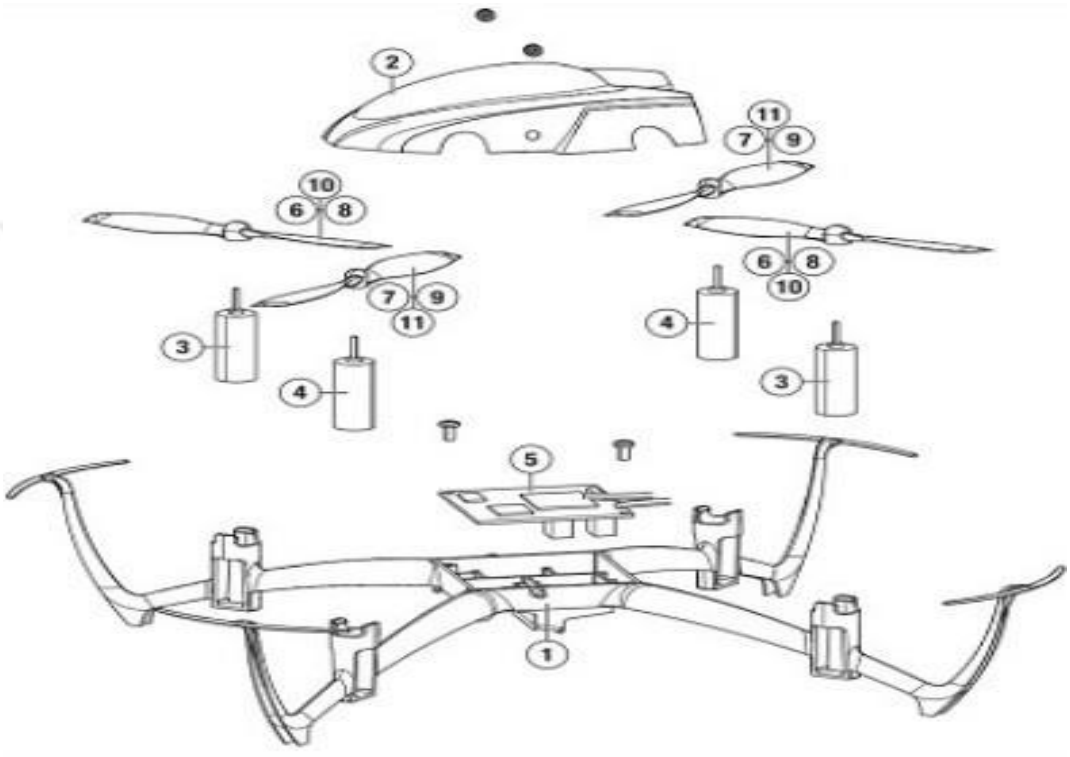
İHA, kelimesi genellikle literatürde ''Drone'' ya da UAV/UAS (Unmanned Aerial Vehicle/ Systems- İnsansız Hava Aracı) olarak adlandırılmaktadır. Bu araçların içinde herhangi bir kişi bulunmaz. Uzaktan kontrol sağlanır. Bir yolcu taşıma işlemi sağlanmaz. Verilen görev karşılığında lazer, kamera gibi araçları taşıyabilen, uzaktan kontrol edilebilen bir uçak türüdür (Özfındık, 2021, s. 428).

Tarihsel gelişime baktığımızda ilk uzaktan kumandalı hava araçlarının tarihi çok eskilere dayanmaktadır. 22 Ağustos 1849 tarihinde ilk İHA kullanımı sağlandı. Avusturyalıların dönemin şartlarını sonuna kadar kullanarak içinde zaman fitili olan 200 adet bombayı pilot olmadan balonlar sayesinde, Venedik şehrine başarılı bir şekilde gönderdi. Bu saldırıda birtakım olumsuzluklarda yaşanmıştır. Bazı balonlar rüzgâr etkisi ile Avusturya'nın sınırlarına geri dönmüş ve kendi bölgelerinde patlamıştır. Diğer bir kısmı ise İtalya'ya ulaştıktan sonra görevini tamamlamış ve patlamıştır. Bu durum İHA'ların kullanıldığı ilk savaş olarak kabul edilmiştir. ABD'de ise kullanımı daha eskiye dayanmaktadır. 1793 tarihinde balonlar ile yaşanılan iç savaşın durumunu görmek adına keşif amaçlı kullanımı olmuş bunun dışına çıkmamıştır.1908 yılında ise bu duruma benzer bir olay yaşanmıştır. 10 Alman balonun içinde yaklaşık 25 havacı, balonlar sayesinde Fransa sınırından geçmiş buraya iniş yapmıştır. Bu durum daha sonra Paris Barış Konferansında görüşülmüş herhangi bir gelişme kaydedilmemiştir. Uluslararası Konferansta bu konunun görüşülmesi, tartışılması insansız hava araçları hakkında ilk diplomatik girişimlerin başladığı yer olmuştur (Kahveci & Can, 2017, s. 512-513).

Dünya genelinde baktığımızda ilk İHA'nın geliştirilmesi 1916 yılında M.low tarafından yapılmıştır. İkinci Dünya Savaşında teknolojinin gelişmesiyle birlikte İHA kullanımı artmıştır. İHA'lar özellikle trenlerin kontrol edilmesi ve korunması hususunda önemli görevler üstlenmiştir. Buradan gelebilecek saldırılara karşı gerekli önlemler alınmıştır. Teknolojide

yaşanılan değişimler ile birlikte İHA yapımında değişikliklerde artmaya başlamıştır. Bu gelişmeler ile ilk jet motorlu İHA, 1951 yılında üretilmiştir. Üretimlerin artması ile İHA'ların kullanım alanları da farklılık göstermiştir. 1955 yılında 1001 İHA modeli yeni bir model olarak ortaya çıkmış, ABD deniz kuvvetleri için kullanılmıştır (Topal, Akpınar, & Beyhan, 2021, s. 19).

Her ne kadar İHA'ya, teknolojik gelişmeler farklı özellikler ve fonksiyonlar eklense de birçok araştırmacı tarafından temel bir İHA'nın genel yapısı ve parçalarının görüntüsü şekil 2.1.1 de verilmiştir.



Şekil 2.1. İHA montaj görüntüsü (Korkmaz , İyibilgin, & Fındık, 2016, s. 105)

Şekilde görüldüğü gibi numaralandırılarak verilen parçaların gövde kısmı, hareket ve elektronik parçaları listelenmiştir. Bu parçaların birçoğu ağırlık gibi etkenlerden dolayı plastik, fiber ve diğer malzemelerden üretilmektedir.

Tablo 2.1. Şekil 2.1.1 'de verilen İHA'nın bileşenleri

NO	**İsim**	**Adet**
1	Gövde	1
2	Üst Koruma	1
3	Sağ Motor	2
4	Sol Motor	2

5	Devre Kartı	1
6-8-10	Sağ Pervane	2
7-9-11	Sol Pervane	2

Şekil 2.1.'de görüldüğü üzere genel İHA üzerinde bulunan parçalar bu şekildedir. Bu parçalar sayesinde hareket etmekte ve verilen görevleri yerine getirmektedir. Tarihte önemli savaşlarında da uzaktan kumandalı olarak İHA kullanılmış, askeri operasyonlarda yer almasına rağmen çok aktif kullanılmamıştır. Yapılan bu tarihsel gelişmeden de görüldüğü gibi yaşanan birçok olay, savaş ve dönemin koşulları İHA'ların kullanımın yaygınlaşmasına neden olmuştur.

2.2. Yönlendirmesi ve Konumu

İHA'ların bir merkezden yönlendirilmesi sonucu hedef gösterilen yeri bazı yöntemler ile bulunabilmektedir. Burada İHA için yönlendirmeler keşif veya organizasyon bölgesinde ki yerin konumunu bünyesinde bulundurduğu teknoloji ile merkeze aktarabilir.

İHA için hedef gösterilen yerin bilgileri merkeze aktarılırken verilerin kısa sürede ulaştığını ve doğruluk konusunda en ideal seviyede olduğu kabul edilmektedir. İHA tarafından herhangi bir yanlışlığın olmaması adına gündelik hayatta sıklıkla karşılaştığımız Global Positioning System (GPS- Küresel Konumlama Sistemi) teknolojisine ihtiyaç vardır. Kullanılan bu yöntem dışında sıklıkla kullanılan diğer yöntem İteratif Kalman Filtreleme. Bu yöntem ile sistemlerin sağlamış olduğu avantajlardan yararlanarak GPS- INS Ataletsel (Inertial) Navigasyon Sistemi kullanılarak, Doğrudan Algılayıcı Yöneltilmesi sistemleri ile İHA'lar için avantaj sağlamış ve konum bilgisi elde edilmiştir. INS sistemi aslında Inersiyal Navigasyon Sistemi olarak açıklayabiliriz. Bu teorinin açıklanması Newton'un bir yerde hareket halinde cisimin gücü, sitemde yer alan doğrusal ivmelerin yanında yerçekimin göstermiş olduğu kombinasyon ile yapılır (Atak & Aksu, 2004).

2.3. İHA Sensörleri

Uzaktan kumanda sayesinde uçabilen ve gelişmiş sensörleri sayesinde olumlu, olumsuz tüm hava koşullarına ortam sağlayabilen İHA kendi içerisinde birçok avantaj barınmaktadır.

Herhangi bir zaman diliminde İHA çalışabilir. Bu çalışmayı yapabilmesinde; kızılötesi, termal, kimyasal birçok sensörün İHA'lara monte edilmesi tüm koşullarda kendi içerisinde sınıfının ve askeri envanterin bir numarası olmasını sağlamıştır. Bu sensörler sayesinde sadece gündüz değil aynı zamanda gece de görüntü ve bilgi aktarımı yapılmasına olanak sağlamıştır (Yılmaz Ü. , 2019, s. 43-54).

İHA'lara monte edilmiş gelişmiş geniş açılı kameralar sayesinde hedef gösterilen yer, üç boyutlu haritalandırılması sağlanılır. Bu sensörler ile istenilen alan hızlı bir şekilde taranır. Gerekli yerin hızlı ve seri bir şekilde taranmasıyla zaman ve emek açısından avantaj sağlanır (Sökmen, 2022, s. 68).

İHA'lar sensörler sayesinde birçok işlem sağlayabilirler. İHA'ya entegre edilecek gelişmiş bir sensör veya kamera ile yüz tanıma işlemi yapılır. Bu işlem sayesinde suçluların kimlik tespiti sağlanıp, yakalanmaları beklenenden daha kısa bir zamanda gerçekleşir. Yüz tanımanın dışında suçlu silah ya da kesici bir aleti varsa bu sensörler sayesinde bulunup gerekli önlemler alınır. Bu sayede İHA'lar ve SİHA'lar keşif ve gözetleme dışında tehlikeli olabilecek durumlar karşısında, sensör ve kameraları sayesinde gerekli önemlerin alınmasını sağlar (Burgaz, 2020, s. 95).

İHA kendi alanında sağladığı avantajlar olarak önemli bir konumdadır. Özellikle gelişmiş sensörlerin ile avantaj sağlamaktadır. Sensörler verilen görevlere göre farklılık göstermektedir. Kızıl ötesi ve gaz sensörlerinin bulunması gece olan olaylarda avantajı artırmaktadır. Sınıfına göre büyük İHA'lar radar sensörleri kullanabilirler. Hava durumunun çok kötü olması durumunda ise İHA sensör olarak Sentetik Aralıklı Radar (SAR) kullanabilir. Bulunan bu sensörler görevlerin zorluğuna göre değişiklik gösterebilir (Baştürk, 2015, s. 79). Önemli bazı sensörler şekil 2.2 ve 2.3'de verilmiştir;

Şekil 2.2. Lidar (Katrancı, 2020, s. 11)

Kendi sınıfı içerisinde önemli bir yere sahiptir. Üzerinden bulunan lazer ışınları sayesinde Lidar, cisimleri taramaktadır. Sensörlerden çıkan lazer ışınları sayesinde dik bir açıdan yönlendirilmekte ve kayıt alınmaktadır. Lidar'a göre daha yakın mesafelerin ölçülmesinde ise

Termal Kızılötesi (FLIR) ve Yakın Kızılötesi (NIR) kullanılır. Termal IR sayesinde nesnelerin özellikleri belirlenmektedir (Katrancı, 2020, s. 11).

Şekil 2.3. CCD TV (Katrancı, 2020, s. 12)

Özellikle gündüz İHA'lara monte edilmesiyle siyah-beyaz ya da renkli görüntü alabilmektedir. Yüksek bir maliyete sahip olmasına rağmen ağırlıkları diğer sensörlere göre daha düşüktür (Katrancı, 2020, s. 12).

2.4. Hareketleri

İHA veya diğer hava araçları bazı yönelimler doğrultusunda hareket eder. Bunu sağlarken de özellikle sahip olduğu bazı durum açıları vardır. Bu avantajları kullanarak saha içerisinde kendisine alan yaratır.

İHA ve SİHA gibi hava statüsünde yer alan araçların üç tane durum açısı bulunmaktadır. Bu yönelimleri kullanarak işlemler sağlanır. Bu hareketler; baş açısı, yuvarlanma açısı ve yunuslama açısı olmak üzere üç tanedir. Baş açısında, aracın burun kısmının hareketleri dikkate alınır. Sağa dönüş hareketi, pozitif olarak algılanırken sola dönüş ise negatif olarak adlandırılır. Yuvarlanma açısında ise burun kısmında ziyade kanat uçlarının hareketleri önemsenir. Aşağı ve yukarı yapılan yönelimler dikkate alınır. Açının tamamen sıfır olması ile kanatların yatay konumda olduğu bilinirken, sağa taraflı yapılan bir hareket pozitif olarak

değerlendirilir. Son olarak yunuslama açısında diğer hareketlerden farklı aşağı ve yukarı yönlü yönelimler bulunur. Burun kısmının aşağı temaslı bir hareketi olumlu yorumlanırken tersi bir hareketi negatif olarak değerlendirilir (Katrancı, 2020, s. 16).

2.5. Aerodinamik Açıları

İlk geleneksel İHA'lar, kullanılmaya başlandığında bazı zorluklar ortaya çıkmıştır. Özellikle kanatları konusunda sabit durum gösteren İHA'ların kanatları küçültülmüştür. Bu durum sahip olduğu aerodinamik yapının bozulmasına sebep olurken ve havada kaldığı süreyi uzatmıştır. Bunu yapabilmesi için özellikle hızını artırması gerekmektedir. Bu aerodinamik yapıdan dolayı sabit kanatlı İHA'lar kullanım açısında geri planda kaldı. Kanat alanında olan bu negatif durumu ortadan kaldırıp daha yüksek hızlarda çalışmasına ihtiyaç vardır (Yılmaz, Keiyinci, Çam, & Karcı, 2017, s. 1036).

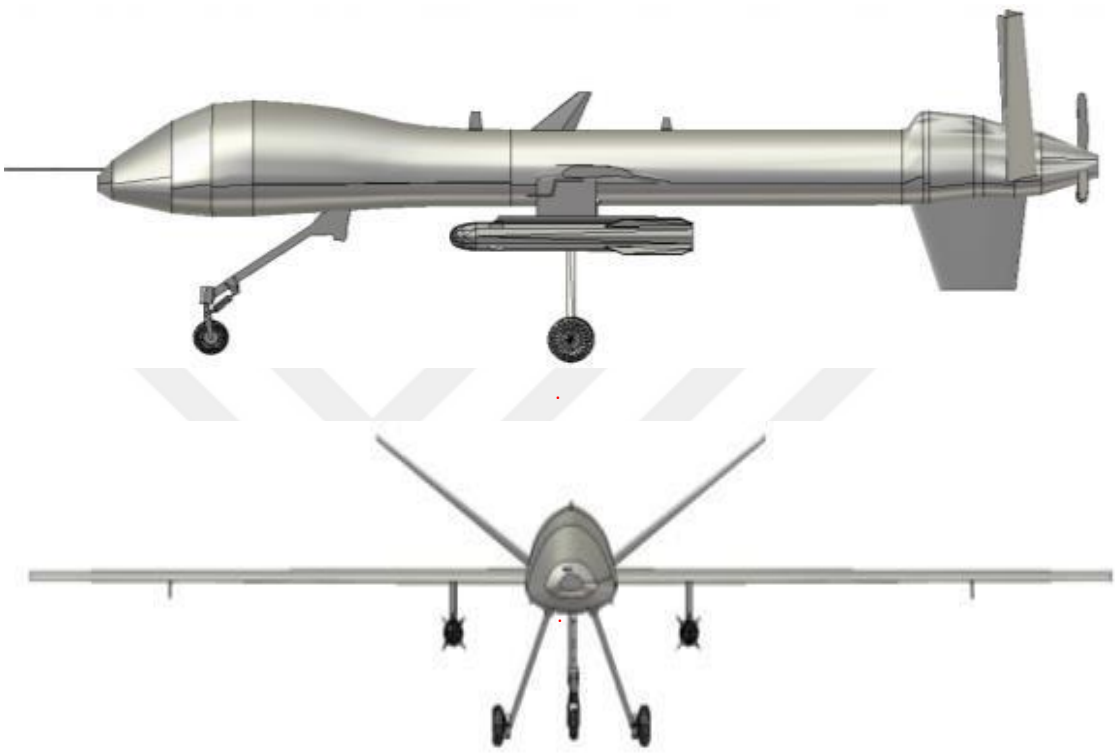
Yeni yöntemler ile beraber aerodinamik alanlarda elde edilen verimler artmaya başlamıştır. İHA'lar da şu an iki tane aerodinamik açı bulunmaktadır. Bunlar; yana kayış ve hücumdur. Bu acıların özellikleri her ikisinde de gerçek hava hızının arasındaki farkından faydalanmaktadır. Hücum acısında, gerçek hava hızının yunuslama açısından farkına bakılmaktadır. Yana kayış açısı ise daha farklı olarak gerçek hava hızından, baş açısı arasındaki farktan elde edilmektedir (Katrancı, 2020, s. 17).

2.6. SİHA

Silahlı insansız hava araçlarının gelişmesi ile birlikte bu araçlara olan güvenirlik artmaya başlamıştır. Özellikle silahların bu araçlara monte edilmesi ve kullanılması, devletlerin dikkatini çekmesini sağlamıştır. Bu silahların kullanılmasıyla birlikte askeri alanlarında önemli başarılar elde edilmiştir. Devletler bu başarılardan sonra SİHA konusunda kendilerini geliştirmeye başlamışlardır. Askeri alanda sağlayacağı avantaj ile ilerleyen yıllarda SİHA'nın kullanımı artacaktır. SİHA kullanımında ki bu artış, özellikle silahlanma konusunda rekabet ortamının oluşmasına neden olacaktır. Çünkü askeri alanda kendisini, SİHA konusunda geliştiren devletlerin adından sıkla bahsedilmeye başlanmıştır. Bu rekabet ortamı bazı devletler şimdiden kendisini göstermektedir.

Düşmana karşı saha üstünlüğün ele geçirilmesi konusunda sınıfında bir numaradır. Çünkü gözetleme yapıldıktan sonra sahip olduğu silahlar ile bu düşman birliklerin yok edilmesini sağlayabilir. Bu silahlar olmasaydı normal askeri birliklere veya savaş uçaklarına ihtiyaç duyulabilirdi. SİHA sayesinde askeri malzemelerin kullanımın en aza indirmesi ile düşmanlarına karşı üstünlük kurmuştur. Kendisine monte edilmiş silahlar ile mürettebat olmadan verilen askeri görevleri yerine getirmiştir. Bu sayede savaş unsurlarının tüm çevresini değiştirmiştir. Özellikle SİHA'lar diğer savaş silahlarından farklı olarak kontrol

edilebilme özelliği vardır. Uzaktan kontrol ve erişim sayesinde sahada askeri personele ihtiyaç duyulmaz. Elde edilen bilgilerin istasyona aktarılmasından sonra gerekli tüm işlemler sağlanır.



Şekil 2.4. Temsili SİHA modelinin fiziksel olarak yandan ve önden görünüşü (Nişancı, Teşneli, & Teşneli , 2018, s. 392)

Savaş esnasında SİHA kullanmayı alışkanlık haline getirmeye başlayan devletler, bazı avantajları da kendileri için yaratmış olmaktadırlar. Bu avantajlara kullanıcı veya askeri kişilerin ölümünün azalması yanında ülkeler için sağladığı prestijler unutulmamalıdır. Diğer askeri teçhizatlara göre daha ekonomik olması devletlerin SİHA kullanımında bazı ana nedenlerdir (Küçük, 2022, s. 60).

SİHA'ların özellikle insan kontrolünde olan bir savaş uçağına göre daha fazla havada kalabilme süresinin yanında, hedef tanımlaması yaparken ortam içerisinde yer alan zaiyatların az olması konusunda daha başarılıdır. SİHA bir noktaya ya da bölgeye bir saldırı aşamasında olacaksa bunun karar verme süreci karar vericilerin dışında kullanıcılar ile birlikte yapılır (Ak & Avaner, 2019, s. 47).

SİHA teknolojisine her ne kadar devletler tarafından kullanılmasına olumlu bakılsa da dünya kamuoyunda ciddi eleştiriler vardır. Bu olumsuz söylemelere karşı, 2013 yılında Birleşmiş

Milletler İnsan Hakları ve Temel Özgürlüklerin Korunması ve Geliştirilmesi ile ilgili raporu, Özel Raportör Genel Kurulu sunmuştur. Bu raporda; özellikle SİHA'ların çatışma ve askeri alanlarda büyük faydalar sağladığı dile getirilmiştir. Çatışma içerisinde kalan sivillerin ölüm oranlarındaki azalmalardan raporda sıklıkla belirtilmiş ve birçok olumlu değerlendirmeler yapılmıştır (Ak, 2018, s. 116). Şekil 2.5, 2.6. ve 2.7'de günümüzde önemli bir yere sahip SİHA'lar bulunmaktadır.

Şekil 2.5. MQ-9 Reaper ABD SİHA (Karakuş, 2019, s. 58)

MQ-9 Reaper, 14 saat uçuş görevi gerçekleştirebilirken 1.5-ton mühimmat taşıma özelliğine sahiptir. Saatte 482 km hıza kadar çıkabilen MQ-9 Reaper, sensörleri sayesinde geniş alanlarda sinyal istihbaratını sağlayabilmektedir. Bu özelliği kullanabilmesinde sahip olduğu kızılötesi ve ısıya hassas sensörlerin etkisi büyüktür. Görev yaptığı konumda gizli yapılan telefonları ya da telsiz telefon gibi iletişim araçlarıyla yapılan konuşmaları dinleme özelliğine sahiptir. Bu özelliklerinin yanında belirlenen konuma isabetli atış kabiliyeti ile verilen görevleri eksiksiz yerine getirebilmektedir (Karakuş, 2019, s. 58).

Şekil 2.6. Bayraktar TB2 Türkiye SİHA (Düz, 2022, s. 12)

Türk yapımı olan Bayraktar TB2, Sahip olduğu sensörlerin yanında taksi, kalkış, seyir, iniş ve park gibi seyir kabiliyetine sahiptir. Uçuş görevi 18.000 feet operasyonel irtifa alarak 27 saat havada kalabilmektedir. 150 kg ağırlık taşıma ve 4 adet lazer güdümlü akıllı mühimmat taşıyabilir. Uçuş esnası sırasında sağlamış olduğu görüntü aktarma ve arşiv özelliği sayesinde görüntüler izlenebilir sonrasında aktarımlar sağlanabilir. Sağlamış olduğu bu özellikler ile Katar, Ukrayna, Azerbaycan gibi ülkelere ihraç edilmiştir. İhraç edilen ilk hava aracıdır.

Şekil 2.7. Wing Loong II Çin SİHA (Birer, 2022, s. 72)

İlk defa 2005 yılında Wing Loong I modeli başlayan Çin, 2015 yılında Wing Loong II olarak geliştirdiği üst modeli ortaya çıkardı. Sabit kanat modeli ile radar sitemlerinde yakalanma olasılığını en aza indirmiştir. Yaşanacak herhangi bir saldırıda, füze ve lazer güdümlü bomba kullanabilir. Bu özellikleri ile ülkelere ihraç edilmektedir (Birer, 2022, s. 72).

2.7. SİHA'ların Tarihi

Birinci bölümde İHA'ların tarihsel gelişimine yer verdik. Buna ek olarak teknolojinin gelişmesiyle birlikte askeri alanlarda yapılan değişiklikler SİHA'ların gelişmesine neden olmuştur. Aynı şekilde SİHA'ların tarihi bu şekilde başlamış oldu. İHA'lar ile yaşanan birçok gelişme SİHA'ları da etkilemiştir. Bu sayede SİHA araçları çıkmış ve devletler tarafından kullanılmaya başlanmıştır. İHA'larda yer alan gözetleme ve keşif yeteneğinin SİHA'lara entegre edilmesi ile birlikte birçok terör operasyonlarında aktif görevler üstlenmiştir.

11 Eylül'de dünya gündemini ve ABD devletini derinden etkilemiştir. Bu terör saldırısından sonra Afganistan işgalini başlatan ABD, İHA'ları aktif kullanmaya başladı. Burada yapılan silahlandırma çalışmaları SİHA için bir dönüm noktası oldu. Bunların yanında SİHA'larda yer alan istihbarat ve silah kullanma özelliği ile birçok olayda etkili bir şekilde görevini başarı ile yerine getirdi. İHA'ların terörizmde kullanılmaya başlanmasıyla birlikte, SİHA'lar Afganistan ve Irak operasyonlarında ABD devleti tarafında kullanıldı.2003 yılında ABD tarafından düzenlenen Irak operasyonunda Predator adlı keşif aracı kullanılmış ve silahlandırılmıştır. ABD, Irak için operasyon yapmadan bu araçtan gelen bilgileri analiz etmiş daha sonrasında orduya ait güçler Irak için operasyon başlatmıştır. Yine bu dönemde özellikle İHA'ların coğrafi koşullar bağlamında mayınların temizlenmesi ve sağlık malzemelerin tedarik edilmesi konusunda ciddi yardımları olmuştur (Katrancı, 2020, s. 18).

ABD tek buralarda değil başka ülkelerde de SİHA kullanımına devam etmiştir. 2004 yılında CIA tarafından El Kaide, Taliban unsurları için Pakistan'da SİHA kullanımını aktif bir şekilde sağlamıştır. Bu sistem sadece ABD tarafından değil başka ülkeler tarafından da kullanılmaya başlanmıştır. İngiliz ordusu 2007 yılında Afganistan'da kullanmış iken 2008 yılında İsrail Gazze de SİHA kullanımı sağlamıştır (Akyürek, 2012, s. 7).

İHA ve SİHA'lar birçok coğrafyada aktif bir şekilde kullanılmıştır. Öncelikle keşif ve istihbarat noktalarında İHA kullandıktan sonra bunlara ek olarak karşı birliklerin yok edilmesi için SİHA kullanımı sağlanmıştır. Merkezi İstihbarat Teşkilatı (CIA), NATO gibi önemli kuruluşlar birliklerinin desteklenmesi ve hedeflerin yok edilmesi sürecinde SİHA kullanımını aktif sağlamıştır. Bu dönemde kalmayarak ilerleyen tüm dönmelerde SİHA kullanımı birçok kurum ve kuruluş tarafından kullanılmıştır.

2.8. SİHA'ların Hedef Takibi

Teknolojinin son yıllarda daha fazla gelişme göstermesiyle birlikte özellikle SİHA, hedefin dinlenip, takip edilmesini sağlayarak komuta merkezine iletir. Gelen bilgiler doğrultusunda hedef takibi sağlanır. Son durumda düşman olduğuna karar verildiği anda ise SİHA hedefin yok edilmesi için harekete geçer. Bunları yaparken uzun sürede havada kalarak uygun manevra kabiliyetleri gibi birçok hassas sistemleri vardır.

Ülkeler artık askeri alanlarda hata payı insana göre daha düşük, her türlü zorluğa karşı dayanıklılık gösterebilen İHA veya SİHA ile çalışmaktadırlar. Otonom çalışma özelliğinin yanında yapay zekâ ile gelişme sağlayan bu makineler birçok zorlu görevin üstesinden gelmiştir. Sensör sistemleri sayesinde birçok hedefi çoklu ve anlık takip etmeleri ile operasyonlarda kolaylıklar sağlamıştır. Bu hususta İHA ve SİHA'lar düşman birliklerinin sensörleri sayesinde takip ederek komuta merkezine bilgiler gönderir. Komuta merkezinden gelen onay neticesinde düşmana karşı saldırı yapılır (Mevlütoğlu, 2018, s. 9).

Yapılan hedef takibinin önemli kısmını oluşturan yer kontrol istasyonun temsili olarak aşağıda gösterilmiştir. Burada bir monitor yardımıyla İHA ve SİHA tarafından aktarılan görüntüler, görevli kişi tarafından izlenmektedir. Önünde bulunan joystick ve kontrol düğmeleri sayesinde kontrolü sağlar. Müdahaleye ihtiyaç duyulduğu anda ise gerekli işlemleri hemen başlatır.

Şekil 2.8. Yer Kontrol İstasyonu (Karakuş, 2019, s. 59)

SİHA veya İHA'lar sadece hedef takibi yapmazlar. Bunun dışında düşman birliklerin sinyal takibinin yapılması, haberleşme için kullanılan cihazların dinlenilmesi, radar sistemlerinden karşı görünmez olması özelliği ile birçok özelliği kendi içerisinde bulundurur. Sahip olduğu yapay zeka sayesinde uzun sürede hedef takibinin yapılması, iniş ve kalkış durumlarının sağlanması, operasyonların yöneltilmesi gibi süreçlerin sağlanması konusunda SİHA ve İHA'lar sınıfının en iyisidir (Caner, 2013, s. 226).

2.9. SİHA'ların Sınıflandırılması

SİHA sınıflandırması konusunda birçok farklı yorum bulunmaktadır. Bu yorumlar devletler, kurumlar ve kişiler tarafından yapılmıştır. ABD, NATO, Avrupa Sivil İHA Yol Haritası, JAPCC ve JUAS COE tarafından bu araçların teknik ve sistemsel özelliklerine bazı sınıflandırmalar yapılmıştır. Karaağaç (2016)'ın ise İHA sınıflandırması konusunda kullanım ve kullanıcı bazlı olarak bunu sağlamıştır.

Tablo 2.2. İHA Sınıflandırma (Karaağaç , 2016, s. 32)

İHA Sınıfı	**Kullanım Seviyesi**	**Asli Kullanıcı**	**Diğer Kullanıcılar**
Mikro	Tek Personel/ Tim	Özel kuvvetler ve İstihbarat Örgütleri	Kara ve Deniz Kuvvetleri, Deniz Piyadeleri
Mini	Tek er, tim, manga takım, bölük ve tabur, tek gemi	Kara ve Deniz Kuvvetleri, Deniz Piyadeleri	Hava Kuvvetleri
Küçük	Alay ve tugay, deniz görev grubu	Kara ve Deniz Kuvvetleri, Deniz Piyadeleri	Hava Kuvvetleri
Taktik	Kolordu ve ordu, deniz görev kuvveti	Kara ve Deniz Kuvvetleri, Deniz Piyadeleri	
Operatif	Harekât Alanı	Hava Kuvvetleri	Kara ve Deniz Kuvvetleri, Deniz Piyadeleri
Stratejik	Harekât Alanı	Hava Kuvvetleri	İstihbarat Örgütleri

Tablo 2.3. NATO İHA Sınıflandırma (Katrancı, 2020, s. 21)

Sınıf	Kategori	Uçuş İrtifası (Metre)	Görev Menzili(km)	Veri İletim
1.Sınıf (150 kg)	Mikro<2 kg	<610 m (Yerden)	5 km	LOS
	Mini 2-20 kg	<915 m (Yerden)	25 km	LOS
	Küçük>20 kg	<1524 m (Yerden)	50 km	LOS
2. Sınıf (150-600 kg)	Taktik	<3048 m (Yerden)	200 km	LOS
3. Sınıf (> 600 Kg)	Male	>13716 m (Deniz seviyesinden)	Sınırsız	BLOS
	Hale	<19812 m (Deniz seviyesinden)	Sınırsız	BLOS
	Savaş	<19812 m (Deniz Seviyesinden)	Sınırsız	BLOS

NATO dışında ABD ise farklı sınıflandırmalar ve yorumlamalar kullanmış olsa da Joint Unmanned Aircraft Systems Centers of Excellence (JUAS COE) tarafından özellikle sahip olduğu ağırlık, yapabileceği hız ve irtifa noktalarında sınıflandırmada bulunmuştur.

Tablo 2.4. ABD İHA Sınıflandırma (Katrancı, 2020, s. 21)

	Maksimum Kalkış Ağırlığı	Uçuş İrtifası	Seyir Hızı (Km/h)
1.Grup	<9	<366 M (Yerden)	<185 Km/h
2.Grup	9.5-25	<1067 (Yerden)	<463 Km/h
3.Grup	<599	<5488 (Deniz Seviyesinden	<463 Km/h
4.Grup	>599	<5488 (Deniz Seviyesinden)	Her Hız
5.Grup	>599	<5488 (Deniz Seviyesinden)	Her Hız

Diğer bir sınıflandırma ise Avrupa Sivil İHA tarafından yapılmıştır. Bu sınıflandırma da SİHA'ların kalkış ağırlığı ve alabildikleri irtifalar hakkında yapılmıştır. Bu tarz sınıflandırmalar hem İHA hem SİHA'lar için yapılmaktadır.

Tablo 2.5. Avrupa Sivil İHA Yol Haritasına Göre İHA Sınıflandırması (Katrancı, 2020, s. 21)

	Kalkış Ağırlığı (Kg)	**Uçuş İrtifası (Metre)**
Mikro	<7	<122
Mini	8-400	92-1220
Döner Kanatlı		
Male	400-4000	4572-13716
Male		>13716

Şekillerde görüldüğü üzere birçok sınıflandırma yapılmıştır. Yapılan sınıflandırmalar SİHA ve IHA için önemli olup bu hususlarda değerlendirmeler yapılmıştır. Özellikle NATO, ABD ve Avrupa Sivil İHA Yol haritası tarafından yapılan sınıflandırmaların günümüz teknoloji ile incelendiğinde eski bir sınıflandırma olduğu açıktır. Yapılan sınıflandırmalarda öncelikli olarak en güncel olanından başlanmıştır.

2.10. SİHA'ların Kullanım Alanları

SİHA özellikle son yıllarda birçok farklı alanda kullanılmaya başlandı. Yoğunlukla kullandığı alanlara istinaden bazı sınıflandırmalar yapılmıştır.

-Özel görevler: Birçok görev içerisinde desteği alınan SİHA'lar özellikle haberleşmek için destek sağlaması, mayınlı bölgelerin bulunup sonrasında imha edilmesi, arama ve kurtarma faaliyetlerine katılması gibi birçok özel görevde yer almıştır.

-Elektronik Harp: Bazı önemli harplar bulunmaktadır. Radar, muharebe, önleyici elektronik harp gibi.

-Hedef Benzetimi: Özellikle sahte uçak benzetiminin yapılması.

-Taarruz: İç güvenliğin sağlanması, taarruz esnasında hava sistemlerinin yok edilmesi veya hava savunma sistemlerinin savunulması.

-Keşif ve Gözetleme Desteği: Saha alanlarının keşfi ve öncesinde gözetlenip stratejik desteğin sağlanması.

-Kirletici Görevler: Kimyasal veya nükleer tehditlerin bulunduğu ortamlar İHA ve SİHA için tehlike arz etmez.

-Tehlikeli Görevler: Çok önemli ve tehlikeli görevlerde, uçakları kullanan görevlilerin hayati tehlikeleri olmadığı için göreve odaklanma durumu daha fazladır. Uçak düşse dahi sonrasında herhangi politik krize ya da mürettebat kaybına neden olmaz.

-Uzun Süreli Görevler: SİHA ekibinde yer alan kişilerin yer kontrol istasyonunda vardiyalı çalışarak, görev süresi uzun olan olaylarda gözetlemenin daha dikkatli ve verimli olmasını sağlar (SSM, 2017, s. 124).

3. BÖLÜM

YENİ DÜZENDE ÇATIŞMA BİÇİMLERİNDE İHA VE SİHA

Canlılar, varlıklarını devam ettirebilmek için üremenin dışında kendilerini savunmayı öğrenmişlerdir. Hayvanlar bunu kendilerine özgü geliştirdikleri taktikler ile yaparken insan, akıl iradesi ile çevresinden gelebilecek saldırılara karşı kendisini korumaya almıştır. İlk başladığında korunmak için ok ve kılıç kullanan insanlar, teknolojinin zaman içerisinde gelişmeye başlamasıyla birlikte ateşli silahlardan, yazılım ile desteklenmiş silahlara, İHA ve SİHA gibi teknolojilere geçiş yapmıştır.

İnternet alanında yaşanılan teknolojik gelişmeler ile kullanımı artmıştır. Internet kullanımın yaygınlaşması devletlerin ve kurumların güvenliklerini sağlama noktasında sıkıntılar yaratmıştır. Sahip olunan bilgilerin giderek artması ile siber güvenlik alanında devletlerin tedbirler almasına neden olmuştur. Ağ bağlantıları sayesinde başlayan bilgi paylaşımı, küresel birçok sorunu beraberinde getirmiştir. Elde edilen teknoloji, bilgiyi daha yararlı süreçler için kullanım sağladığında İHA ve SİHA gibi araçlar üretilmesi, çatışmaların değişmesine neden olmuştur.

Devletlerin ortaya çıkması ile birlikte askeri alanda gelebilecek tehditlere karşı güvenliklerini sağlama konusunda önlemler almışlardır. Bu durum insanların refahı ve mutlulukları için yapılması gerek en öncül hareketlerden kabul edilmiştir. Özellikle 1.ve 2. Dünya Savaşlarından sonra güvenliğin uluslararası bağlamda sağlanması adına sistemlerin yeniden inşa edilmesine olan ihtiyaçlar artmıştır. Sonrasında yaşanan 11 Eylül saldırıları ise güvenlik alanında derin bir etki bırakırken güvensizlik ortamının artmasına sebep olmuştur. Devlet dışı aktörlerin çıkması, küreselleşmenin hızlı bir şekilde yaşanıp, internet kullanımın artması ile geleneksel savaş algısı da değişmeye başlamıştır. Terör ile mücadele için İHA ve SİHA kullanımını bu sayede artmaya başladı ve devletler bu alanda yatırımlarını arttırdılar. İnternetin ve teknolojinin gelişmesi İHA ve SİHA için farklılıklar yaratırken asıl yeni düzende devletler arasında alanda coğrafi sınırların ortadan kalkmasına sebep olmuştur. Burada sadece internet kullanım artmasının dışında bilgisayar, cep telefonu gibi cihazların kullanımın insanlar tarafından benimsenip kullanılması toplumsal değişimleri beraberinde getirmiştir. İnternetin yaygınlaşması ise birçok değişimin habercisi olmuştur (Eren , Mart 2017).

İHA ve SİHA gibi siber güç olanaklarını çatışmada kullanabilmek için siber uzay faaliyetlerinde etkin rol almak önemlidir. Siber güçte devletler diğer savaş alanlarındaki gibi bu alanda kendilerini göstermek ve avantaj sağlamak istemektedirler. Siber uzay veya siber güç olanakları ile devletler bunu yapmaya çalışmaktadır. Örneğin ABD Hava Kuvvetleri Temel Doktrininde, siber uzay ile ilgili tanımlar bulunmakta çatışma alanları hakkında bilgiler içermektedir (Yıkıcı, 2020, s. 8).

Askeri gücün yanında devletlerin artık siber güç ile birlikte taraflara karşı zarar verebilecek olması veya korkutmak amacıyla siber saldırıların kullanılması yeni çatışma biçimlerini oluşturmuştur. İHA ve SİHA gibi teknolojiler, bunun için bir araç olarak kullanılmıştır.

3.1. Değişen Dünyada İHA ve SİHA

Ateşli silahların insansızlaştırılması ve savaş alanlarında askeri teçhizatların kullanan görevli kişilerin yerine artık otomatik, uzaktan kumandalı silahlar geçmiştir. Bu yöntem ile çatışmalarda askeri kayıpları en az seviyeye indirgemiştir Yapılan savaşlarda bir cephe statüsünün kalmamasının yanında değişen dünya koşullarında, silahların insansızlaştırılması birçok sorunu da beraberinde getirmiştir. Uluslararası ilişkilerde bu alanda yaşanan gelişmeler beraberinde yaptırımlar, hukuki kararlar ve yeni savaş biçimlerinin doğmasına neden olmuştur

Savaş ve yapısı hakkında başlayan çalışmalar özellikle, eski sistemlerin kullanılmamasına neden olmuştur. Eskiye göre yeni sistemlerin daha çok kullanılmasında teknolojinin gelişerek silah alanında farklılığını ortaya çıkarması etkili olmuştur. Özellikle İHA ve SİHA teknolojisinin aktif olarak kullanılmasıyla birlikte bu durum değişmiştir.11 Eylül saldırılarından sonra Afganistan ve Irak işgallerinin yanında Suriye, Libya, Yemen, Suudi Arabistan gibi ülkelerde yoğun olarak SİHA ve İHA teknolojisine yer verilmiştir. Bu silahların kullanılmasında değişen savaşlar koşulları ve teknolojini ne kadar aktif kullanıldığını açıkça ortaya koymaktadır. SİHA ve İHA'ların çatışmalarda keşif yeteneğinin olması, gözetlemeden sonra düşman birliklerinin imha edilmesini sağladı. Bu özellikleri sayesinde kullanan devletler tarafından taktik ve operasyonel üstünlük elde edilmiştir.

Devletler, artık uluslararası ilişkilerde özellikle yakın dönem ilişkilerinde, çatışmalarda kendileri için vekil bulmaktadırlar. Vekalet savaşları olarak adlandırılan bu olayda devletler genel olarak daha çok terör örgütü olan gruplara doğudan ve isteyerek askeri yardım (araç, gereç, mühimmat) yapar. Devletler bu sayede dış politikada daha etkin rol oynar. SİHA ve İHA'ların artık terör örgütlerinde kullanılması savaş alanlarında sadece devletin değil şiddet eğilimi yüksek olan devlet dışı aktörler tarafından kullanılması da bu grupların teknolojik süreçlere açık olduğunun göstergesidir (Yeşiltaş & Duran, 2018).

Tablo 3.1. Şiddet Eğilimli Devlet Dışı Aktörler ve Terör Örgütlerinin SİHA Kullanımı (Bergen, Salyk-Virk, & Sterman, 2020)

ÖRGÜT	KULLANDIĞI YIL	KULLANILDIĞI YER
Peşmerge	-	Suriye, Irak
Aum Şinrikyo	1993	Japonya
Kolombiya Devrimci Silahlı Güçleri (FARC)	2002	Kolombiya

Hizbullah	2004	İsrail, Suriye
Hamas	2010	İsrail
Libyalı İsyancılar	2011	Libya
El-Kaide	2013	Pakistan
Donetsk Halk Cumhuriyeti	2015	Ukrayna
Horasan Ordusu	2015	Suriye
Suqour al-Sham Tugayları	2015	Suriye
Şam Lejyonu	2016	Suriye
DAEŞ	2016	Suriye, Irak
Taliban	2016	Afganistan
Türkistan İslam Partisi	2016	Suriye
Jalisco Yeni Nesil Karteli	2017	Meksika
Husiler	2017	Suudi Arabistan
Libya Ulusal Ordusu (Hafter Bağlısı)	2017	Libya
Maute Grubu	2017	Filipinler
PKK	2017	Türkiye
Boko Haram	2018	Nijerya
Heyet Tahrir El Şam (HTŞ)	2018	Suriye
Venezüella Ordu Firarileri	2018	Venezüella

Değişen dünyada özellikle insansız ve silahlı hava araçlarının gelişmesiyle birlikte bu araçlarının kullanımı artış göstermiştir. Bunu sadece devletler değil onların yerine görevler üstelenen terör unsurları da yapacaktır. Modern dünyada yaşanılan değişimler bu araçlara olan ihtiyacı artıracak ve yaşanılan birçok çatışma da üstün görevler alacaktır

İlk İHA kullanımı her ne kadar Avusturyalılar tarafından yapılsa da ilk uzaktan kumandalı İHA 1918 yılında Birinci Dünya Savaşında ABD tarafından havalandırılmış ve güvenli olarak iniş yapmıştır.914 metre boyunca uçuş yapan Curtis N-9 Aerial Torpedo modeli İHA diğer devletler tarafından da dikkat çekmiştir. İngiltere, Almanya gibi devletler savaşlarda kullanmak üzere İHA geliştirmeye başladılar. Birinci ve İkinci Dünya Savaşları'nda kullanılan İHA modelleri diğer savaşlarda aktif rol alacağının göstergesidir. Keşif, gözetleme, istihbarat gibi amaçlar ile kullanılmaya başlanılan İHA'lar daha sonrasında silahlandırılmasıyla SİHA kullanımı başlamıştır. Devletlerin özellikle engebeli ve arazi şartlarının kötü olduğu yerlerde birçok İHA ve SİHA kullanımı sağlamıştır (Erdağ, 2020, s. 14).

SİHA ve İHA'nın bu şekilde aktif olarak kullanılmasında en önemli sebeplerin başında istenilen hedefi net olarak bulması ve aktarabilmesidir. İHA ve SİHA genel olarak askeri ve sivil görevler için kullanılmış önemli görevler üstlenmişlerdir. Savaş dışında kullanıldığı birçok alan vardır. Sosyal ve eğlence dışında, bilimsel araştırmalar, yeni yapılacak hava tahminleri, okyanuslar ile alakalı genel bilgilerin toplanması, arkeolojik kazıların incelenmesi, doğal afetlerden sonra oluşan hasarın tespiti, kentsel dönüşüm gibi birçok durum ve olay için kullanılabilir. Bugün ve gelecekte İHA ve SİHA, sıcak ve soğuk iklimler dışında okyanusda dahil birçok ortamda çalışmaya devam edecektir. Performanslarının daha iyi olması konusunda Ar-ge çalışmaları her gecen gün artmaktadır.

3.2. İHA ve SİHA'larda Yaşanabilecek Sorunlar

İHA ve SİHA üzerinde yer alan kameralar sayesinde görüntüler bir istasyon sayesinde bilgisayara aktarılmaktadır. Görüntüler sayesinde görevler başlatılır. İHA ve SİHA da bu görevler sırasında bir pilot bulunmaz. Uçaklara yapılacak herhangi bir saldırı sonrasında pilotun bulunamaması diplomatik gerginliklerin daha kısa süreli sürmesini sağlar. Uçuşun otomatik pilotlar ile yapılmasının yanında, İHA ve SİHA da yer alan sensörlerin ağır ve büyük olması onlar için dezavantajdır. Yapılacak uçuşlar öncesi kontrolleri sağlamak amacıyla birçok yazılım ve mobil uygulamalar yapılmıştır. Bu sistemler sayesinde bağlantılar yapılmaktadır.

İHA ve SİHA' da yer alan dahili hafıza bilgileri kaydetmektedir. Bu verilere uçuş sonrasını ulaşılabilmektedir. Bu verilere ulaşma hızı yapılan uçuşların süresi ile doğru orantılıdır. Eğer kolluk kuvvetleri tarafından bu bilgilere ihtiyaç varsa İHA ve SİHA'larda anlık veri iletme özelliğinin bulunması gerekir. Çünkü kolluk kuvvetlerinin kullanacakları istihbarat, keşif gibi durumlarda görüntülerin bir yere aktarılması yeterli gelmeyebilir. Bilgilerin başka bir noktaya aktarılmasına ihtiyaç duyulabilir. İHA ve SİHA'nın bu noktada ağ üzerinden bilgi aktarımı ve paylaşımı çok önemlidir. Bu paylaşım yapılırken siber tehditlere ve karşı taraftan gelebilecek sinyallere karşı dikkatli olunmalıdır. Aksi takdirde yapılacak herhangi bir siber saldırı görevin başarısız olmasına, İHA ve SİHA'nın düşmesine ya da bilgilerin değiştirilerek görevlerin yerine getirilmesi engellenebilir. Aynı şekilde sinyaller arasında yaşanabilecek bir karışıklık sonucu kazalar oluşabilir hava trafiği aksayabilir. Bunlardan ötürü güvenlik güçlerinin siber tehditlere karşı yüksek güvenlikli İHA ve SİHA kullanmalıdır.

Bu hava araçlarında sistem ve teknoloji bütünleşmesi sağlanamaz ise ciddi sorunlar oluşabilir. Özellikle kentsel alanda kullanılacak İHA ve SİHA'larda çarpışmayı önleme veya algılama özelliği bulundurulmaya bilir. Ancak devletler için hayati öneme sahip, şehir merkezinden uzakta olan enerji boru hatları için mutlaka İHA ve SİHA'larda algılama sisteminin yanında çarpışmayı önleme olmalıdır. Dışarıdan yapılacak saldırılara karşı hava olaylarını da göz aradı

etmemek gerekir. Uçuşa başlandığı anda yaşanılacak bir türbülans İHA ve SİHA'larda görevlerin tehlikeye girmesine yol açmakta bulunun verilerin korunmasını zorlaştırmaktadır. Sadece veriler konusunda değil silahların kullanılması zorluklar yaşanırken sensörlerin hareketlerinde önemli bozulmalar yaşanabilir. Yaşanılacak olumsuz hava koşulları veya türbülans bunların dışında direk İHA ve SİHA'nın parçalanmasına da yol açabilir.

3.3. İHA'lara Yönelik Siber Saldırılar

İHA aracı oluşturulurken her bileşeni için ayrı bir montaj ve teknoloji ihtiyacı vardır. Bu montaj işlemi sağlanırken farklı güvenlik açıkları oluşabilir. Bu açıklar özellikle donanım, yazılım, ağ bağlantısı, sensör ve haberleşmeden kaynaklı olabilir. Bu güvenlik açıkları devletler için ciddi sorunlar oluşturabilir. İHA'nın bileşenlerinin bulunduğu genel yapısı tablo 4.2'de verilmiştir.

Tablo 3.2. İHA'yı Oluşturan Temel Bileşenler (Coşar, 2022, s. 260)

Donanım	**Yazılım**	**Sensör**	**Ağ Bağlantısı**	**Haberleşme**
Bilgisayar	İşletim Sistemi	Hızlanma veya ivme	Kablosuz Ağ (WLAN)	Radyo
Tablet	Telemetri	Jiroskopik	Araçlar Arası İletişim (VANET)	Wİ-Fİ
Akıllı Telefon	Güvenlik Yazılımı	Hareket	Mobil Geçici Ağ	Bluetooth
Kamera	Otonom Sürüş Yazılımı	Seviye	Kablosuz Sensör Ağı (WSN)	Kızılötesi
GPS	Yer Kontrol Yazılımı	Basınç	Mobil İletişim için Küresel Sistem (GPS)	Hücresel Bağlantı
Denetleyici	Uçuş kontrol Yazılımı	Kızılötesi	Uydu	
Anten	Diğer Uygulamalar	Görüntü		

Bu özelliklere sahip İHA'lar kendi arasında iletişim kurabilir. Bu iletişim Ad- Hoc ile sağlanır. Ad-Hoc, ağ bağlantıları ve herhangi bir yönlendirme almadan iletişim kurulabilmesini sağlayan cihaz veya düğümdür. Bu düğümler ile doğrudan iletişim kurulabilir. Wİ-Fİ bağlantısı, kızılötesi gibi teknolojik bağlantılar sayesinde yapılabilir (Yalçın & Boyacı, 2020, s. 29). Bu düğümlere gelebilecek herhangi bir saldırı birçok olumsuzluğun oluşmasına sebep olabilir. IHA' ya gelebilecek saldırlar tablo 3.3'de gösterilmiştir.

Tablo 3.3. İHA'nın Ağ Bağlantılarına Karşı Yapılabilecek Saldırılar (Coşar, 2022, s. 262-263)

Saldırı Tipi	**İsim**	**Açıklama**
Aktif Saldırılar	Ortadaki Adam	Karşılıklı iletişimin sağlandığı sırada gizlice bu iletişimin içine sızılarak yapılan saldırı biçimidir. Saldırganın iletişimi dinlemesiyle beraber banka hesapları, kişisel bilgiler ele geçirilip değiştirilmesidir. Burada saldırgan karşılıklı iletişim sağlayanlardan birinin yerine geçmeye başlayıp onun gibi davranır
Aktif Saldırılar	Solucan Deliği	İş birliği içerisinde olan kötü niyetli düğümler, birbirleri arasında iletişim seviyesi yüksek bir kanal oluşturur. Ulaştırılmak istenilen bilgiler bu kanal üzerinden toplanılır. Bu bilgiler bazen değiştirilerek ulaştırılır. Bazende hedefe ulaştırılmaz.
Aktif Saldırılar	Kara Delik	Şifrelemesiz haberleşme esnasında iki düğüm arasında saldıran düğüm, değişiklik yapabilir. Herhangi bir kara delik saldırısında ağ içerisindeki yönlendirmelere kötü niyetli düğüm, isteklere olumsuz yanıt verebilir. Elde ettiği bilgileri silebilir ya da fark edilememek için sadece bilgileri dinleyip hedefe ulaştırabilir.
Aktif Saldırılar	Yönlendirme	Saldırgan genel ağ yapısının işleyişini engellemek ve karışıklara neden olmak için yapılan yanlış yönlendirme saldırıları ile düğümleri hedef alır. Bunu da uykusuz bırakma veya yeniden oynatma gibi saldırıları ile sağlar.
Aktif Saldırılar	Kesme	Düğümler arasındaki iletimi engellemek için yapılır. Hedef düğüme olan erişimin ortadan kaldırılması için saldırgan, yönlendirme mesajların genel içeriğini değiştirebilir. Burada ki amaç kaynak ve hedef düğüm arasındaki iletişimin engellenmesidir.

Aktif Saldırılar	DoS (Hizmet Reddi Saldırısı)	Bu saldırı türünün amacı, ağ ve düğümün koordineli çalışmasını engellemektir. Bunu yaparken de bant genişliğini gereğinden fazla tüketilmesini sağlayarak, CPU, disk ve bellek alanlarının zorla kullandırılmasıyla bu kaynakların tüketilmesi sağlanılır.
Aktif Saldırılar	SYN Saldırısı	Hizmet reddi saldırı türlerinden biridir. Sistemin kullanabileceği veri sınırının üstünde iletişim sağlayarak ağa ve düğüme SYS gönderilmesidir.
Aktif Saldırılar	Kaba Kuvvet Saldırısı	Parola ve kullanıcı bilgilerin olduğu sisteme giriş yapılabilmesi için birden fazla giriş denemesi ile yapılan saldırılardır. Saldırının hemen gerçekleşebilmesi parola ve kullanıcı adının zorluk seviyesine göre değişiklik göstermektedir.
Aktif Saldırılar	Doğum Günü Saldırısı	Bir içeriğin ya da yazılımın doğrulanması amacıyla farklı kombinasyonların oluşturularak yapılan saldırılardır. Saldırgan burada birbirinden farklı şifreler ve kullanıcı adlarını sisteme gönderir. Bu sayede aynı oluşturulan mesaj veya parolanın bulunması amaçlanır. Elde edilen bilgilerin sonradan değiştirilmesi durumunda fark edilemez.
Pasif Saldırılar	Gizli Dinleme	Saldırıyı gerçekleştiren kişi ve kişiler ağ üzerinden olan konuşmaları dinler. Elde edilen bilgilerin analizlerin yapılmasını sağlar.
Pasif Saldırılar	Değiştirme	Paketlerin yanlış yere yönlendirmesiyle ağ üzerinden dolaşmasına ve en sonunda süresinin dolmasıyla ağdan düşmesine neden olur. Ağ içinde sürekli gereksiz yere dolaşan paketler belli bir zaman sonra bant genişliğinin tükenmesine neden olacaktır.

Tablo 3.3'de görüldüğü gibi İHA'lara gelebilecek saldırılar genel bir sınıflandırma dahilinde gösterilmiştir. Bu saldırı türlü aktif ve pasif saldırı olarak ayrılmaktadır. Aktif saldırılar, genel amacı İHA'nın çalışmasını engellemektir. Bunu yaparken gizlilik, bütünlük, kullanabilirlik gibi ihlal edebilecek saldırılar yapar. Bu saldır türleri ise: Ortadaki adam, solucan deliği, kara delik, yönlendirme, kesme, Dos, SYN saldırısı, kaba kuvvet saldırısı ve doğum günü saldırısıdır. Pasif saldırılar ise, gizliliği bozmak için yapılan saldırılardır. Bu saldırı türünde İHA için çalışmasına engel olacak bir durum bulunmamaktadır. Gizli dinleme ve değiştirme bu saldırı türüne örnektir (Coşar, 2022, s. 262). İHA ve SİHA'yı siber saldırılar dışında etkisiz hale getirebilecek

bazı durumlar vardır. Radyo frekansı karıştırma, GPS karıştırma, aldatma, lazer, ağ, silah ve çoklu müdahale yöntemi buna örnektir.

-Radyo Frekansı Karıştırma: İHA konusunda kendini güçlendirmek ve gelebilecek tehlikelere karşı savunma oluşturmak için üreticiler tarafından satışa sunulan bir üründür. Görevli ile İHA arasındaki bağlantının kesilmesi sonucunda drone inişe geçer ya da ilk başladığı alana geri gider. (Sütçüoğlu & Alay, 2019, s. 6) Otonom kullanılan İHA araçlarına karşı ise bu yöntem başarılı değildir. Sistemsel olarak otonom araçlarda haberleşme olanağı bulunmadığı için herhangi bir etki gösteremez.

-GPS Karıştırma: Uydudan alınan GPS sinyalinin İHA ve SİHA'ya ulaşmasını engelleyerek görevin başarısız olmasına neden olur. Sinyal kesildiğinden dronlar geri döner ya da olduğu konuma iniş yapar (Mutlu Genç & Erciyes, 2020, s. 39).

-Aldatma: Uzaktan kontrol edilebilen İHA ve SİHA'lar almış olduğu sinyallerin taklit edilmesiyle kontrolünü kaybeder. Kontrolden çıkan İHA ve SİHA yanlış konumlara yönlendirilerek var olan görevin başarısız olması sağlanılır (Sütçüoğlu & Alay, 2019, s. 7).

-Lazer: İHA ve SİHA araçlarının önemli parçalarına lazer ışığı yönlendirilerek düşürülmesi sağlanılır. Özellikle görüntü iletilmesi sağlayan çipin yoğun ışığa maruz bırakılması ile kameranın bozulması veya görüntünün iletilmesini engelleme amacı bulunmaktadır. Diğer sistemlere göre daha pahalıdır (Mutlu Genç & Erciyes, 2020, s. 39).

-Ağ: İHA ve SİHA görev esnasında iken ağ atılarak pervanenin durması sağlanarak drone düşer ve görev başarısız olur. Çok aktif kullanılan bir yöntem değildir.

-Silah: Görevde olan drone silah yardımı ile düşürülmesi amaçlanır. Bu sayede görev başarısız olur. Diğer yöntemlere göre daha tehlikelidir. Silah ile drone düşürme sırasında seken mermiler veya drone parçaları insanlara zarar verebilir (Sütçüoğlu & Alay, 2019, s. 7).

-Çoklu Müdahale Sistemi: Birden fazla yöntemin kullanılması ile İHA ve SİHA araçlarının devre dışı bırakılması sağlanılır.

3.4. Yeni Dünya Düzeninde Güvenlik Anlayışında SİHA'ların Önemi

Büyük devletler savunma sanayisinde bağımsız olmayı amaç edinmişleridir. ABD, İngiltere, Fransa gibi devletler bu konularda kendilerini geliştirmişlerdir. Savunma sanayilerinde yer alan yüksek teknoloji, yazılımlar ve firmaların bunu üretip satması devletlerin ekonomilerinde ve askeri alanlarda başarılı olmasını sağlamıştır (Tanrıverdi, 2014, s. 3).

İHA ve SİHA üretimlerin yapılabilmesi için ciddi yatırımlar yapılmıştır. Özellikle 11 Eylül saldırısı, 2003 yılında Afganistan işgali gibi durumları İHA ve SİHA kullanımını artıran önemli gelişmeler olarak sıralayabiliriz. Gelecek yıllarda SİHA kullanımı, önemi her gecen gün daha da

artacaktır. Terör örgütlerinin SİHA gibi araçlara karşılık vermesinde yetersiz kalması bu araçların gelecek dönemlerde devletlerin güvenliklerini sağlama konusunda vazgeçilmez unsurlardan biri olacaktır.

İHA ve SİHA'lar bu ortam içerisinde uzun sürede havada kalması ile birlikte ikmale ihtiyaç duymadan gerekirse güneş enerjisinden faydalanılarak uzun süre görevler yapabilir. Güvenlik sağlama konusunda farklı rollere sahip olabilirler. Her ne kadar görevleri kalkışa geçmeden bilgilendirilmiş olsa da uçuşlara başlandığı anda farklı görevler verilebilir.

SİHA'lar güvenlikleri sağlama konusunda bazı karar alıcılardan etkilenir. Tek başına tüm operasyondan sorumlu değildir. Askeri karar alıcılar, politik karar alıcılar gibi kişiler yapılacak operasyonlarda sorumlu kişilerdir. Bu kişiler olumsuzluklar durumunda yetki ve sorumlulukları dahilinde kamuoyuna hesap vermektedirler. Karar vericiler sivil halkın korunması, askeri olarak hedeflerin ayrılması ve yönetilmesi konusunda önemli görevler üstlenmişleridir (Çaycı, 1995, s. 70).

Çatışmaların başlanması veya operasyonlarda SİHA'ların kullanılması konusunda karar verme yetkisine sahip politika yetkilisi kişiler vardır. SİHA kullanımın veya güvenliklerin sağlanması konusunda meşruluk oluşturmak için karar verilmesini sağlar. Diğer karar alıcılardan beklentiler de bu şekildedir. Örneğin pilot ve operatörler yakın karar alama mekanizmalarından biridir. Alınan kararların savaş kurallarına uygun davranışlar sergilenmesi ve yurttaşlarının güvenliklerini sağlama konusunda önemli görevler üstlenmişlerdir.

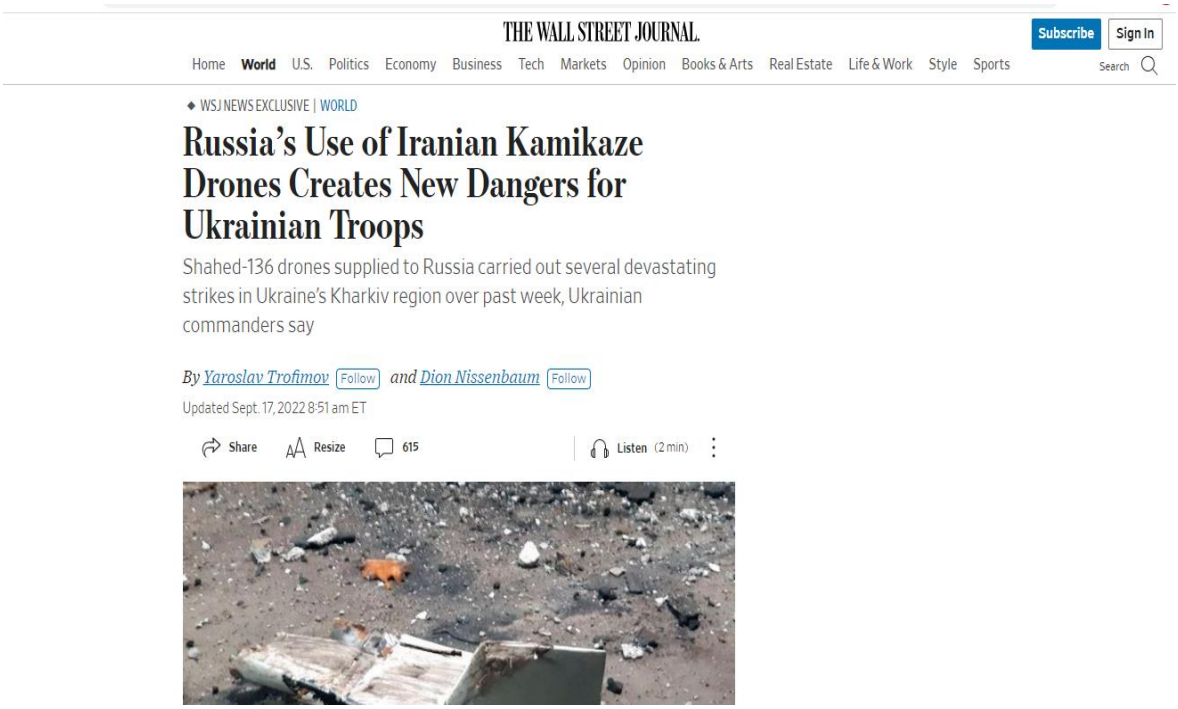
İHA ve SİHA da istihbarat bilgileri anlık olarak komuta merkezine aktarılır. Bu durum savaş stratejisinde önemli kazanımlar elde ettirir. Bu sistemlerin savunmasız tarafı ise karşı taraftan gelen elektronik saldırılardır. Buradaki elektronik saldırılar sayesinde amacı bilgileri komuta merkezine ulaşmadan zarar vermeyi amaç edinir. İHA ve SİHA bu esnada sistemlerin kör edilmesi veya ele geçirilmesi gibi olaylar ile karşılaşabilmektedirler (Ceylan, 2010).

SİHA ve İHA gibi araçlar ilk başta bilgi toplamak amacıyla ile geliştirilmiş olsa da yaşanılan teknolojik gelişmeler ile farklılıklar göstermeye başlamıştır. Uzun süre havada kalması ve sahip olduğu silahlar sayesinde oldukça önemli görevler üstlenmektedirler. Özellikle SİHA'lar, hava savunma sistemleri konusunda yetersiz olan devletlere karşı çok etkilidirler. Havadan havaya veya havadan karaya ciddi zararlar verebilmektedirler. Terör gruplarına karşı daha aktif olarak kullanılan SİHA'lar, sessiz olması ve nokta atışı yapabilmesi ile düşman askerler için ciddi sorunlar yaratmıştır. İHA ve SİHA gibi araçlar her ne kadar askeri çıkarlar için üretilmiş olsa da zaman içerisinde insanlar da kullanmaya başladı. Devletlerin kullanımı ile bu araçlar için birçok yatırımı yapıldı. Bu yatırımlar sayesinde gelişimleri hızlandırıldı. İHA ve SİHA yaşanılan gelişmeler sonrasında devletler için önemli bir aktör olmuştur. Yeni dönemde saldırı ve strateji alanlarında ülkelerin vazgeçilmez unsurları olacaklardır.

3.5. Savaşın Seyrini Değiştiren İHA ve SİHA Haberleri

SİHA ve İHA kullanan ülkeler kendilerini diğer devletlere karşı bu alanda daha avantajlı hale getirmektedir. İHA ve SİHA'nın askeri olaylarda verilen görevleri eksiksiz yerine getirmesiyle, sivil ve askeri kişilerin hayatlarını tehlikeye atmayarak başarılı şekilde çalışmalar sağlamaktadır. Maliyetini az olup elde edilen verimin yüksek olması hükümetler tarafından olumlu karşılanmaktadır. Önümüzdeki yıllarda İHA ve SİHA önemi giderek artış gösterecek ve devletler tarafından daha sıklıkla kullanılmaya başlanılacaktır.

Buna örnek olacak birçok durum bulunmaktadır. İHA ve SİHA kullanımı artık savaşın gidişatını değiştiren önemli unsurların başında gelmektedir. Bu durum bazı devletler için avantaj sağlarken diğer devletler için yıkıcı bir etki yaratır. ABD merkezli Wall Street Journal haber sitesinde yer alan haberde İHA ve SİHA kullanımın sağladığı avantaja vurgu yapılmıştır.



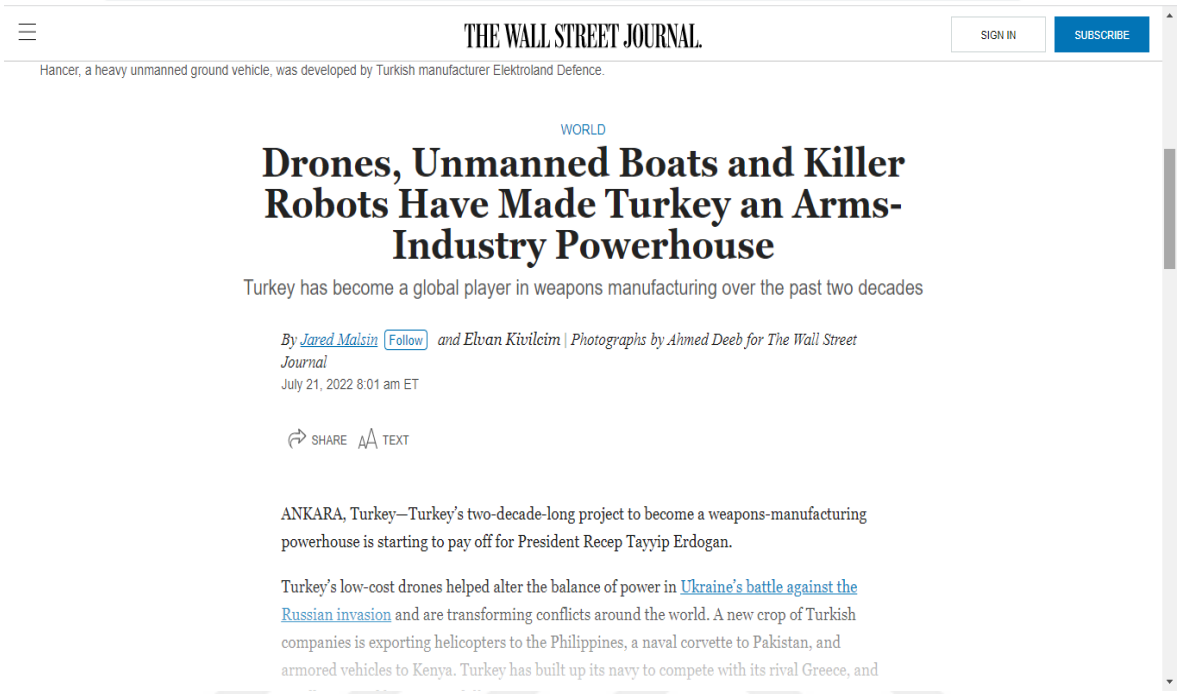
Resim 3.1. The Wall Street Journal Web Sitesi (Trofimov & Nissenbaum, 2022)

Haberin başlığında'' *Rusya'nın İran Kamikaze İHA'larını Kullanılması Ukrayna Askerleri İçin Yeni Tehlikeler Yaratıyor. Rusya'nın kullanmış olduğu Shahed-136 insansız hava aracının Rusya-Ukrayna savaşında Ukrayna'nın Kharkiv bölgesinde birçok saldırı düzenlediği ve yıkıcı etkiler bıraktığı dile getirmiştir. Haberin devamında ise Rusya'nın savaş başladığı andan itibaren ilk kez yabancı silah sistemlerinin konuşlandırıldığını ve Ukrayna kuvvetlerine ciddi zararlar verdiği''* konusu üzerine durulmuştur.

Rusya ve Ukrayna savaşını önemli kılan ve savaşın seyrini değiştiren diğer durum ise Türkiye tarafından sağlanmıştır. Günümüz şartlarında artık İHA ve SİHA kullanımı devletlerin askeri güçlerini artırırken savaşlarında uzamasına sebep olmaktadır. Yine Wall Street Journal 'ın

başka bir haberinde bunu dile getirmiştir. *''Drone'lar, İnsansız Botlar ve Katil Robotlar Türkiye'yi Silah Sanayi Gücü Yaptı"* ifadesini kullanmıştır.

.

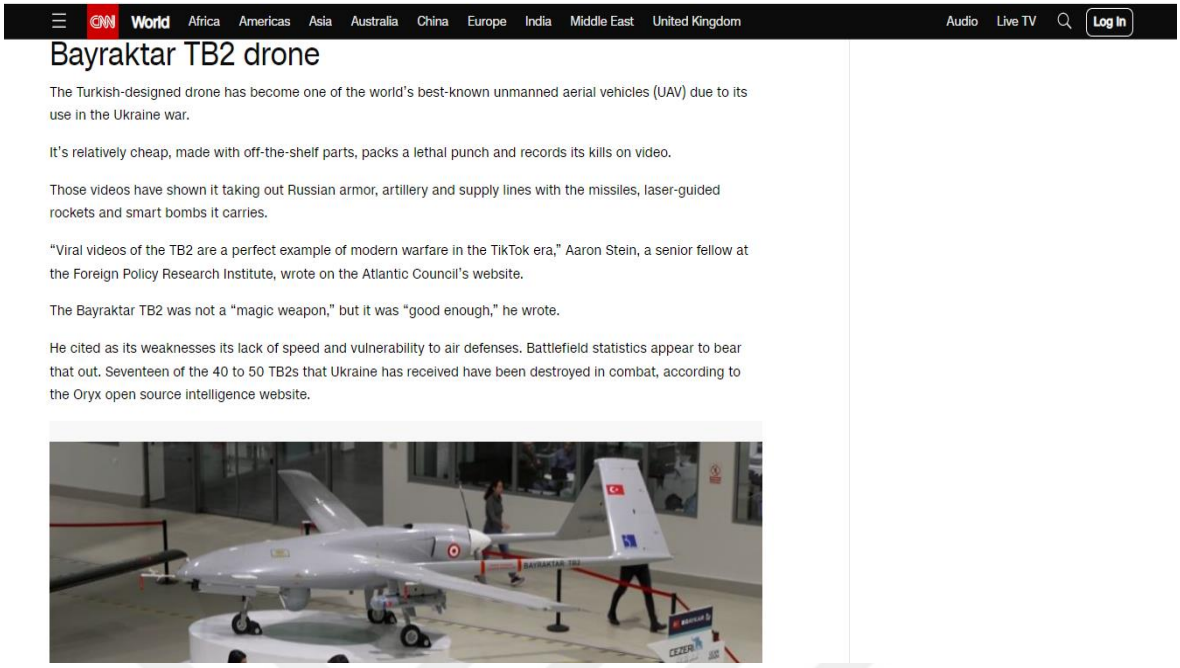


Resim 3.2. The Wall Street Journal Web Sitesi (Malsin & Kıvılcım, 2022)

Haberde yer alan başlıkta *''Türkiye'nin ürettiği ve maliyetinin düşük olan İHA ve SİHA'ların, Rusya'nın Ukrayna işgalinde yaşanılan bu savaşta güç dengelerinin değişmesine yardımcı olmuştur. Türkiye'nin bu sayede silah üreten bir devlet olarak güç elde etmeye çalıştığını dile getirmiştir. Haberin devamında Türkiye'nin, Filipinler'e helikopter, Kenya'ya zırhı araçlar ihraç ederek devletler arasındaki rekabet ortamında adından söz ettirmektedir''.* Yorumu ile İHA ve SİHA satışında Türkiye'nin önemli bir aktör olduğuna değinilmiş ve Rusya, Ukrayna savaşında yaşanılan süreçte Türk İHA ve SİHA'ları aktif görevler üstlendiği vurgusu yapılmıştır.

İHA ve SİHA kullanımı devletlerin uluslararası ilişkilerde aktif gücünü belirleyen önemli unsurlardan biridir. Bu araçların satışı ile ülke ekonomisi ve savunma sanayisinde yeni yatırmalara açacağı olanaklar ile birçok faydası bulunmaktadır. Başka ülkelerden alınabilecek olan İHA ve SİHA araçlarının artık Türkiye'den temin edilmesi bu hava araçlarının diğer devletlere göre üstün özelliklere sahip olduğunun göstergesidir.

RF ve Ukrayna savaşında yapılan CNN haberinde ise: Savaşın uzamasında Ukrayna'nın sağlamış olduğu bazı avantajlar bulunmaktadır. Cirit, Himarlar ve İHA. Bu savaşta özellikle Bayraktar TB2 kullanılması olumlu imajların oluşmasını sağlamıştır.

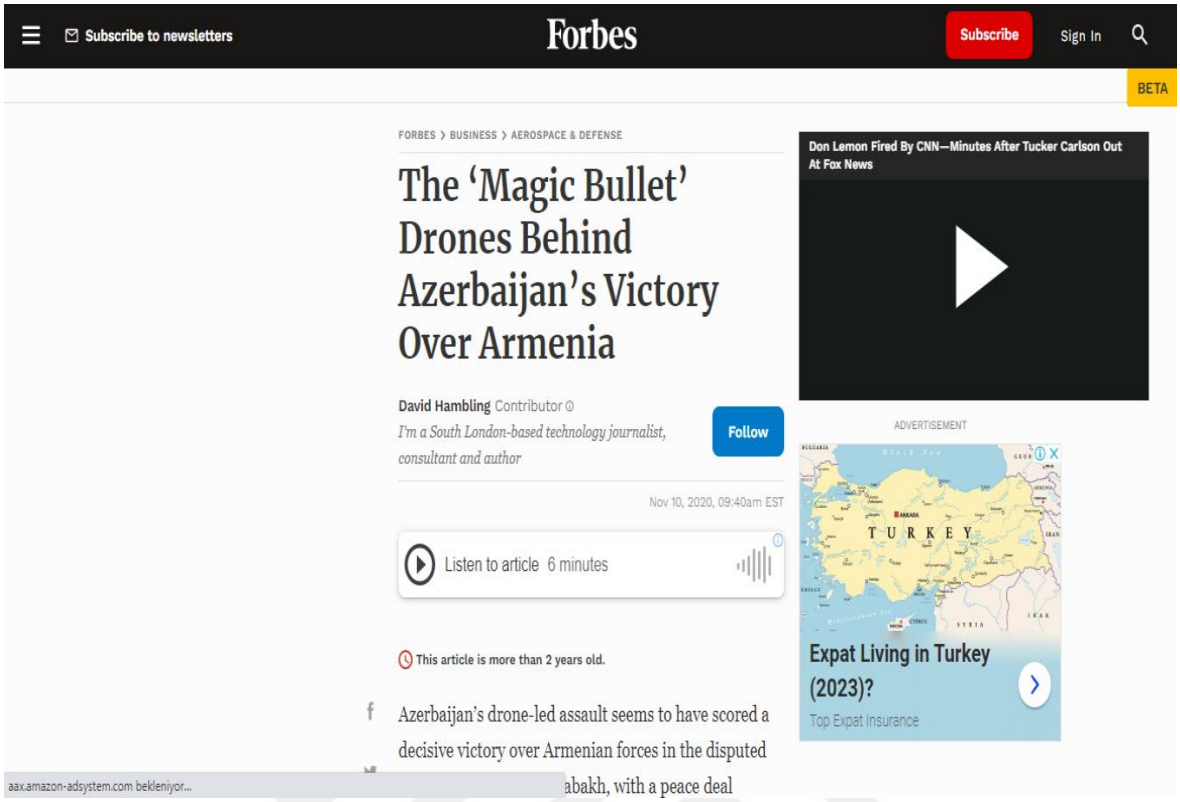


Resim 3.3. CNN Web Sitesi (Lendon, 2023)

Yine haberin devamında *'' Taşıdığı füzeler, lazer güdümlü roketler ve akıllı bombalar ile Rus zırhlarını, toplarını ve ikmal hatlarını etkisiz hale getirdiği* üzerine durulmuştur. *Savaşta kullanılan Bayraktar TB2'nin sihirli bir silah olmadığını ancak yeterince iyi* olduğuna lakin *zayıf yönleri konusunda hız eksikliğine değinilmiş ve hava savunma sistemlerine karşı savunmasızlığından* bahsedilmiştir. *''İnsansız hava araçlarını düşük maliyetinden ve bu savaşta kullanılmasından kaynaklı birçok Ukraynalı pilotların hayatlarını kurtardığı''* haberin devamında yer almıştır.

Yine yakın tarihli savaşlardan biri olan ve Azerbaycan – Ermenistan arasında geçen savaşta İnsanız hava araçlarına Forbes web sitesinde yer vermiştir. Dağlık Karabağ bölgesinde yaşanılan çatışmalarda Azeri insansız hava araçlarının önemine değinmiştir. Bu çatışmalarda Bayraktar TB2 insansız hava araçları yer almıştır. Ermenistan devleti bu savaşı kaybetmiştir. Barış şartlarını kabul etmek durumunda kalmıştır.

Haberde ise *''Azerbaycan'ın Ermenistan'a Karşı Zaferinin Arkasındaki 'Sihirli Kurşun' İnsansız Hava Araçları''* başlığı ile İHA ve SİHA araçlarının öneminden bahsedilmiştir. Yine devamında *Azerbaycan'ın İHA ve SİHA'lar sayesinde tartışmalı Dağlık Karabağ bölgesinde Ermeni güçlerine karşı kesin zafer kazandığını ve barış antlaşmasının yürürlüğüne girdiği* aktarılmıştır.



Resim 3.4. Forbes İnternet Haber Sitesi (Hambling, 2020)

Haberin diğer kısmında ise *Azerbaycan çatışmasında birçok farklı insansız hava aracı kullanıldığı, bunlar arasında en ölümcülleri arasında Türkiye tarafından tedarik edilen Bayraktar TB2 insansız hava aracı yer aldı. ABD ait MQ-9 Peaper'a göre sekizde biri ağırlığında olan saatte 80 mil hızla hareket eden TB2, dört adet MAM (Akıllı Mikro Mühimmat) lazer güdümlü füzeler taşıması diğer İHA ve SİHA'lara karşı etkili olduğunu kanıtlamıştır*.

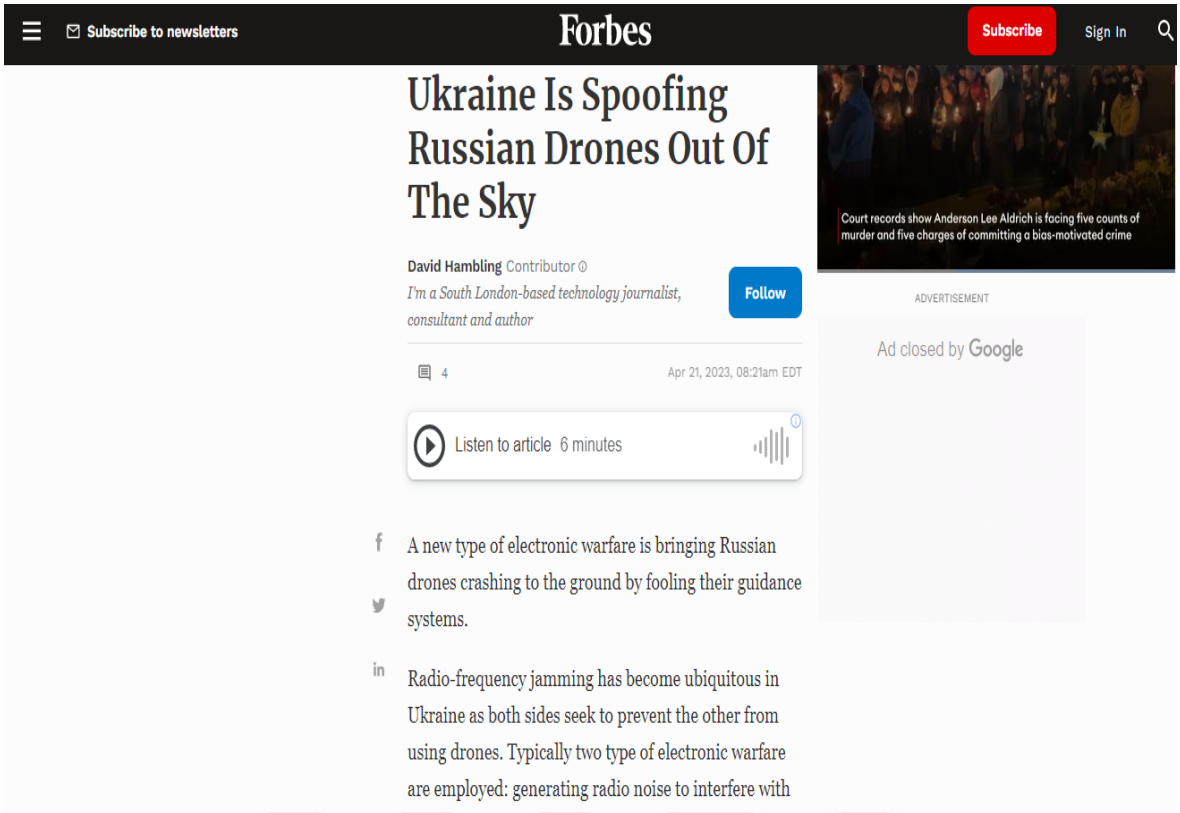
Türkiye dışında İHA ve SİHA satışı yapan devletler bulunmaktadır. Çin, Fransa, ABD gibi devletler hem bu tür savaşlarda İHA ve SİHA satışı sağlamakta hem de askeri envanterini güçlendirip adından söz ettirme cabası içerisindedir. Almanya'da yayın yapan Handelsblatt, internet haber sitesinde geleceğin savaş teknolojisine bu hususta değinmiştir (Resim 3.5.5).

Resim 3.5. Handelsblatt İnternet Haber Sitesi (Jahn, Bomke, Kroll, & Demircan, 2022)

Haberde yer alan başlıkta '' *Hipersonik füzeler, dronlar, yapay zeka: bu teknolojiler silah endüstrisi tarafından kullanılıyor''* ifadesine yer verilmiştir. Haberde yer alan başlıkta gelecekte yapılacak savaşlarda yeni teknolojiler kullanabileceğine değinilmiştir. Dronlar yani İHA ve SİHA teknolojisinin bunda önemli bir görev üstleneceği haber içeriğinde yer almıştır. Dünya genelinde İHA ve SİHA hakkındaki farkındalık düzeyi giderek artış göstermektedir.

Teknolojik olarak üstün olan bu araçlarda bazı noktalarda zayıflıklar bulunmaktadır. İHA ve SİHA teknolojik olarak birçok yapının bir araya gelmesi ile oluşmaktadır. Araçlar üzerinde bulunan kameralar sayesinde görüntüleri aktarılmaktadır. GPS sistemi sayesinde ise düşman birliklerinin konumun bulunması, askeri hedeflerin yok edilmesi gibi gözetleme, istihbarat gibi teknolojik sistemleri içerisinde barındırır. Bu sistemlere gelebilecek siber saldırılar sayesinde İHA ve SİHA araçları çok farklı çalışabilir ve birçok olumsuzluğun başlangıcı olabilir. Ukrayna'nın, Rusya İHA sistemlerine karşı sağlamış olduğu saldırılar buna örnektir.

Forbes dergisinde''*Ukrayna Rus İHA'larını Havadan Kopyalıyor''* ifadesi kullanılmıştır. Haberde yer alan başlıkta, Ukrayna ve Rusya arasında devam eden savaşta İHA sistemlerine karşı yapılan saldırılardan bahsedilmiştir.



Resim 3.6. Forbes İnternet Haber Sitesi (Hambling, 2023)

Haberin devamında ise ''*Rus İha'larının sahip olduğu güdüm sistemleri değiştirilerek imha olunmasını veya yere çarparak parçalanmasını sağlıyor. Yeni bir elektronik harp türü, Rus İHA'larının güdüm sistemlerini bozarak yere çarpmasını sağlıyor. Her iki taraf da diğerinin insansız hava aracı kullanmasını engellemeye çalışıyor. Ukrayna savaşında yaygın hale geldi. Tipik olarak iki tür elektronik savaş kullanılır: kontrol sinyaline müdahale etmek için radyo gürültüsü üretmek, insansız hava aracının pilotluğunu imkansız hale getirmek ve insansız hava aracının uydu navigasyonunun başarısız olması için GPS frekanslarında parazit patlatmak. Şimdi üçüncü bir teknik gözlemlendi: navigasyon sahtekarlığı''.* Bu ifadeler ile İHA ve SİHA sistemlerinin bozulması için yeni bir savaş tekniğinin geliştirildiği ve Ukrayna savaşında kullanıldığı bilgisine yer verilmiştir

Haberde yine ''*Dronlar, uçuşa yasak bölgede olduklarına inandırılarak kandırılmış ve çalışmayı durdurmuşlardır. DJI ve diğerleri gibi dron üreticileri, dron'larının havalimanları gibi yasak alanlarda uçmamasını sağlamak için geofencing olarak bilinen bir yöntem kullanır: tanımlanmış her uçuşa yasak bölgeyi sanal bir çit çevreler ve dron bunun içinde uçmaz''*. Ukrayna bu sayede Rus birliklerine bağlı dronların düşürülmesini sağlamıştır. Yakın zamanda bu tarz haberlerin görülmesi artabilir. Çünkü teknoloji geliştikçe İHA ve SİHA sistemlerindeki açıklar daha çok kullanılmaya çalışılacaktır.

3.6 Uluslararası Alanda İHA ve SİHA'ya Bakış Açısı

3.6.1. AB

İHA ve SİHA konusunda Avrupa Birliği kendi sınırlarında sürekli geliştirme içerisindedir. Hava araçlarını yeni nesil sistemlere uygun hale getirme noktasında yoğun iş birliği içerisindedirler. Bu noktada birliğin iki önemli projesi bulunmaktadır. Bunlardan birincisi Barracuda, diğeri de Dassault nEUROn.

3.6.1.1. Barracuda

Avrupa birliği üye ülkeleri İspanya ve Almanya arasında iş birliği ile geliştirilen bu SİHA, 0,6 Mach hıza ulaşabilen, 200 km mesafe ve 600 metre yükselme kabiliyetini sahip olunacağı düşünülen MALE sınıfı bir İHA'dır. Bu özelliklerinin yanında görünmezlik teknolojisiyle birlikte tam otonom bir sisteme sahiptir.

Şekil 3.1. Barracuda (Katrancı, 2020, s. 82)

İlk test uçuşlarına ise 2 Nisan 2006 tarihinde EADS (Airbus) firmasıyla başarılı bir şekilde gerçekleşmiştir.23 Eylül 2006 tarihinde uçuş esnasında kaza olmasıyla, 2007 yılında bu program durdurulmuştur.2009 yılında tekrar uçuşlarına başlayan Barracuda, 2012 yılına dek uçuşlarına devam etmiştir (Karaağaç , 2016, s. 22).

3.6.1.2. Dassault nEUROn

1999 yılında Dassault tarafından LOGIDUC İHA programı başlatıldı. Programın üçüncü aşamasına gelindiğinde maliyetlerinin çok yüksek olmasından kaynaklı diğer devletlerin bu programa katılmasına karar verildi. Fransa, İsveç, İsviçre, İtalya ve Yunanistan'ın programa dahil olmasıyla, 2003 yılında nEUROn programı başlamıştır. 2006 yılında İspanya'nın da dahil olmasıyla üye ülke sayısı altı olmuştur. Bu ülkelerin katılımıyla birlikte geleceğin SİHA'sının ortaya çıkartılmaya çalışılmıştır. 2010 yılında ilk tasarımı yapıldıktan sonra ilk test uçuşuna 2012 yılında başarı ile tamamlamıştır. Atış testlerinin İtalya'da yapıldıktan sonra programının başarılı bir şekilde tamamlanması beklenmektedir (Karaağaç , 2016, s. 23).

Şekil 3.2. Dassault nEUROn (Katrancı, 2020, s. 83)

2016'da Fransız uçak gemisi Charles De Gaule üzerinde kalkış ve iniş uçuşlarını başarılı bir şekilde gerçekleştirmiştir. İsveç, Fransa, İtalya'da silah ve uçuş testlerine devam etmiştir. Kara, deniz platformlarına iniş yapabilmesini yanında görünürlüğü diğer İHA ve SİHA hava araçlarına göre daha azdır. Teknolojisi geliştirme aşamasında olan bu SİHA da kullanılacak jet

motoru ile hızının 1 Mach'a ulaşılacağı öngörülmektedir. Seri üretime başlaması noktasında ise net bir bilgi bulunmamaktadır (Katrancı, 2020, s. 83).

3.6.2. NATO

Teknolojik gelişmeler ile muharebe sahaları değişmiştir. Gözetleme, keşif ve istihbarat yeteneklerinin kuvvetli olduğu araçlara ihtiyaç duyulmuştur. Gece ve gündüz havada kalmasında sorun olmayan, görüntü aktarabilen, yüksek öldürme oranına sahip, teknolojik araçları NATO da kullanmak istemektedir. Avrupa birliği kendi arasında yaptığı birçok çalışma gibi, NATO örgütü de kendi içerisinde çalışmalarını yapmaktadır**.** Burada yapılan çalışmalar askeri ve savunma alanı üzerine olsa da siber alan, İHA, SİHA gibi alanlarda çalışmalarını yürütmektedir.

Gelecek yıllarda orduların daha güçlü olmasını ve diğer silahlara karşı avantaj sağlama konusunda İHA ve SİHA'ların diğer savaş araçlarına göre bir adım önde olacağı açıktır. Çünkü İHA ve SİHA'ların savaş yöntemlerini değiştirmesi, caydırıcılık seviyesinin diğer silahlardan daha fazla olması, ilerleyen dönemlerde yaşanılacak değişimlere önderlik yapacağını söylemek yanlış olmaz.

NATO da harekatlarında İHA ve SİHA araçlarını kullanmaktadır. 2010 yılında Tunus'ta başlayan ve literatüre 'Arap Baharı' olarak yerini alan isyan olayları birçok ülkeyi etkilemiştir. Yemen, Fas ve Libya bu ülkelerdendi. Orta Doğu'da başlayan ve siyasi yönetimlere karşı olan bu hareketler, Ortadoğu ve Kuzey Afrika'da birçok değişimin başlangıcı olmuştur.

17 Şubat 2011 tarihinde başlayan isyan hareketleri dönemin Devlet Başkanı Muammer Kaddafi tarafında şiddetle karşılık bulmuştur. Yaşanan bu şiddet olaylarının devam etmesi ve Kaddafi'nin iktidarı elinde tutma isteği sonucunda Libya'da aylarca devam eden iç savaş 'ın nedeni olmuştur. Yaşanan iç savaşta Libya halkına yönelik verilen ölümcül karşılık uluslararası alanda büyük tepki toplamıştır. Bu tepkilerin sonucunda bazı kararlar alınmıştır. Birleşmiş Milletler Güvenlik Konseyi (BMGK)'nın 1973 sayılı karar ile Libya için uçuş konusunda yasak alanlar oluşturuldu. Libya'da bulunan halkın korunması amaç edilmiştir (Ok, 2015, s. 112-113).

Libya'da 'insanlığa karşı suç' eylemlerinin artmasıyla birlikte buraya askeri müdahale yapılmasına karar verildi. Yapılan hava harekâtları, Afganistan'a yapılan harekata benzemektedir. Afganistan'daki gibi İHA uçakları önce keşif uçuşları yapıldı. Sonrasında gözetleme ve istihbarat toplanılarak uçuşlara devam edildi. İttifak Kuvvetlerine destek vermek için gözetlenen hedeflerin vurulması için SİHA'lar görev almıştır. Libya Harekâtı'nda yaklaşık 200 SİHA saldırısı yapıldığı düşünülmektedir (Terkan, 2015, s. 53).

Tablo 3.4. NATO'nun Libya Harekâtında Kullandığı İHA Platformları

ÜLKE	**SİSTEM**	**KULLANIM AMACI**
ABD	U2- 1 Adet	Görüntü Sağlama
	E3-B/C Sentry- 3 Adet	Havadan Erken Kontrol ve Uyarma
	E8-C Jstars- 3 Adet	Havadan Satıh Gözetleme
	RC135-V Rivet Joint–1 Adet	Sinyal İstihbaratı
	EP3-E Aries II- 1 Adet RQ4-A Global Hawk- 2 Adet	Sinyal İstihbaratı Havadan Satıh Gözetleme
İngiltere	E3-D Sentry-2 Adet	Havadan Erken Kontrol ve İhbar
	Tornada GR4- 4 Adet	Görüntü İstihbaratı
	Nimrod R1- 1 Adet	Sinyal İstihbaratı
	Sentinel R1- 1 Adet	Havadan Satıh Gözetleme
Fransa	Harfang- 1 Adet	Görüntü İstihbaratı
	E3-F- 2 Adet	Havadan Erken Kontrol ve İhbar
Yunanistan	Embraer R99-A	Havadan Erken Kontrol ve İhbar

2010 yılında başlayan olaylar neticesinde 31 Mart 2011 tarihinde müdahale edilmesine karar verilmiştir. Alınan bu karar neticesinde 31 Ekim 2011 tarihinde harekât son bulmuştur. Bu süre içerisinde NATO birliklerine bağlı ittifak kuvvetleri Libya'da kullanmış oldukları İHA'lar tablo 3.4'de gösterilmiştir (Suscan, 2022, s. 40-41).

Şekil 3.3. NATO envanterine katılan RQ-4 Global Hawk İHA'sı

Savaş durumlarında keşif ve gözetleme kapsamında RQ/MQ-4 Global Hawk ve RQ-170 Sentinel İHA araçları ABD tarafından aktif kullanılmaktadır. RQ-4 Global Hawk İHA'sı 2016 yılında NATO tarafından bünyesinde barındırılmaya başlanmıştır. Önümüzde yıllarda ise askeri ve savunma envanterini güçlendirmek isteyen NATO, İHA ve SİHA alanında yapılan gelişmeleri yakından takip edip alımlar yapmaya devam edecektir (Karaağaç , 2016, s. 36).

3.6.3. BM

Uluslararası alanda birçok örgüt bulunmaktadır. Birçok devlet bu örgütlere katılmışlardır. Evrensel güvenliğe önem veren bu kuruluşlardan en önemlilerden bir tanesi Birleşmiş Milletler'dir. Uluslararası barışın ve güvenliğin devamını sağlamak amacıyla kurulan BM gerek siber alanda gerekse İHA ve SİHA konularında birçok çalışması bulunmaktadır.

SİHA ve İHA'lar ile yapılan operasyonlarda öncellikle teröre karşı güvenliği sağlama ve sivillere zarar görüp görmediği araştırılır. SİHA'lar genellikle terör ile mücadele etmek ve egemenlik ihlallerinde yasal olup olmadığı şu an için belirsizdir. Uluslararası hukuk kapsamında bu konu tartışılmaktadır. Çünkü terör kavramının uluslararası alanda birçok farklı anlamı bulunmaktadır. Hangi olayların terör bağlamında değerlendireceği ve bu saldırılara karşı SİHA ile müdahale edilmesi hususunda hala belirsizlikler bulunmaktadır. Bu belirsizlikler ışığında BMGK onayı olmadan ilan edilecek bir savaş olayında veya terör mücadelesi kapsamında haklı gerekçeler göstererek (jus ad bellum) bir devletin topraklarında SİHA'lar ile operasyonlar

yürütmesi, hem uluslararası hukukun ve devletin egemenliğinin yok sayılmasıdır. Özellikle barışın devamını ve ilerlemesini sağlamak için kuruluna BM'de SİHA'ların sivil, asker veya suçlu olarak ayrım yapmada zorlandığı savaş esnasında sivil insanların ayrımını yapma konusunda zorlandığı için eleştiriler yapılmaktadır (Özerdem, 2021, s. 149).

Haklı gerekçeler gösterilmeden yani savaş ilan edilmeden SİHA'ların kullanılmasına BM tarafından sıcak bakmadığı açıktır. Nitekim İHA ve SİHA gibi araçların kullanımın artmaya başlaması, raporları ve bilim adamları tarafından yapılan çalışmaları da beraberinde getirmiştir. BM, İHA ve SİHA'nın geliştirilmesini kısıtlamak için uluslararası alanda çalışmalar yapmıştır. BM bünyesinden özerk olarak çalışmalarını yürüten, silahsızlanma konusunda uzmanlaşmış kurumu olan Silahsızlanma Araştırmaları Enstitüsü (UNIDIR) tarafından yürütülen çalışmalarda ve raporlarda bu silahlarının kullanımı konusunda endişelerini dile getirilmiştir.

SONUÇ

Teknolojinin gelişmesiyle birlikte internet alanında yaşanılan olumlu değişmeler tehdit unsurlarının da değişmesine neden olmuştur. Bilimsel verilere daha hızlı ulaşmasıyla birlikte ekonomi, siyasi, askeri, kültürel birçok alanda değişimler başlamıştır. Ülkeler bu süreçte kendi aralarında ki sorunları çözmek için kimi zaman savaş kimi zaman da siber alanı tercih etmiştir. Bunun içinde eğitimli askerlere, teknolojik silah ve teçhizatlara ihtiyaç duymuşlardır. Teknolojideki bu değişimler, ulusal ve uluslararası alanda dikkat çekici birçok sürecin de başlangıcı olmuştur. Siber saldırılar ise bu unsurlardan en tehlikeli olanıdır. Çünkü bu saldırı türünde fiziksel engelleme şansı devletler açısından bulunmamaktadır. Devletler bu savaşlara hazırlıklı olmak durumundadır. Bu yüzden birçok devlet siber güvenlik konusunda stratejiler oluşturmayı amaç edinmiştir.

Bilişim ve iletişim alanında yaşanılan süreçler uydu teknolojilerini değiştirmiştir. Uluslararası ilişkilerde kara, deniz, hava ve sonrasında uzay sahasının oluşmasını sağlamıştır. Uydulaşma ve gözlem kapasitesinin küresel çapta kullanılmasıyla, değişimler başladı. Kara, deniz, hava ve uzay sahalarından sonra birbirleri ile bağlantı kurulmasını ve etkisinin daha hızlı gösteren bir alan oluştu. Siber alanın beşinci boyut olarak oluşması ile devletler arasında güç dengeleri farklılaşmaya başladı. Uzayda alınan bilimsel veriler ve artan teknolojik gelişmeler ile insan yapımı sanal bir ortam oluşturulmuştur. Siber alanda yaşanılan gelişmeler ile gerek küresel ilişkilerde gerek insani ilişkilerin oluşmasında belirleyici rol oynadı. Siber alanın daha fazla kullanılması ile bu alanın kapsamı içerisine; bilgisayarlar, ağ sistemleri, yazılımlar, internet, bilgi ve telekomünikasyon, alt yapısal sistemler, akıllı uygulamalar dahilinde birçok yazılım dahil oldu. Aktif kullanılması ile birlikte uluslararası ilişkilerde devletlerin ulusal güvenliklerini etkileyen yüksek politika unsuru haline gelmiştir.

Yeni teknolojiler ile birlikte günlük hayatımız birbirleri ile bağlı olmaya başladı. Ulaştırma, iletişim, finans, iş yaşamı birçok hizmet grupları (kamu ve özel) alt yapılarında bilgi ve teknolojilerden faydalandı. Bu yüzden gizlilik, bütünlük ve erişebilirlik gibi alanlarda siber alana bağımlı hale geldiler. Bilgi teknolojilerinin giderek birbirleri ile daha bağımlı hale gelmesiyle devletler için koruması gereken uluslararası bir konu haline gelmiştir. Elde edilen bilgiler düşman ülkelerin eline geçmesiyle toplumun düzeni bozulabilir ve ekonomik olarak işleyişi engelleyebilir. Bundan dolayı siber alan son yüzyılın en önemli konularından biri olmuştur.

Devletlerin, siber alanda yaşadığı bu değişimler ulusal ve uluslararası güvenlik anlayışında kendisine has siber güvenlik stratejilerinin ve planlamalarının oluşmasına sebep olmuştur. Özel yasalar çıkartıp, devlet kurumlarını bu alanda bilinçlendirerek siber uzayda kendilerini güçlendirmeye çalışmışlardır. Uluslararası güç yarışında yer alabilmek için ulusal güvenlik stratejilerinin oluşturulması gerekli hale gelmiştir. ABD, RF, Çin, Güney Kore, Kanada, Japonya, Singapur, Hindistan, Avusturalya, Birleşik Krallık, İsrail gibi devletler siber uzayda lider olma

yolunda kendi içerisinde yarış haline girmişlerdir. Gelebilecek saldırılara karşı, oluşturdukları ulusal savunma sistemleri burada hayati önem taşımaktadır. Çünkü internet ve ağ bağlantılarına yapılacak saldırı sayesinde kritik alt yapı sistemlerinin çalışması mümkün olmaz. ABD, Çin, RF gibi devletler her ne kadar siber alan konusunda çok güçlü devletler olarak görünse de saldırıya en açık devletlerdir. ABD o yüzden akademik ve resmi evraklarda ''hibrit savaş'' diye bahsederken, Çin ise siber alanda olan hibrit savaşları için ''sınırsız savaş'' söyleminde bulunmuştur. RF, Almanya, İngiltere gibi devletlerinde siber alan konusunda ciddi çalışmaları bulunmaktadır.

Her devlet kendisini siber alanda güvende hissedebilmek için strateji belgesi oluşturmuştur. Siber alanda yaşanılan interdisipliner çeşitlilik ile birlikte devletlerin iç ve dış politikaları etkilenmiştir. Siber alanı, ulusal güvenliğe dair etkili yönetilmesini sağlamak, ulusal ve uluslararası alanda etkili bir yol olacaktır. Bu alanda uzman ekiplerin kurulması, stratejilerini geliştirilmesi, toplumsal değişimlerin başlamasına neden olmuştur. Bu alanda yapılacak saldırılara karşı oluşan istihbarat birimleri uluslararası ilişkiler için devletler adına avantaj sağlayacaktır. Uluslararası alanda devletlerin, aktör olarak varlıklarını ön planda tutma isteği ile siber alanda kendilerine yer edinmeye çalışmışlardır. Uluslararası ilişkilerin doğası gereği zaten bu durum çok zor iken siber alanda ise bu durumu sağlamak imkansıza yakındır. Çünkü, sınırsız ve belirsiz bir alan olan siber uzayda hakimiyet kurmak imkansızdır. Buradaki değişimin ve dönüşümün altın anahtarı, siber ordular ve yaşanılan teknolojik gelişmelerdir.

Tüm bunlar ile birlikte artık 21. yy ile bilgiler, ağ bağlantıları sayesinde birbirine bağlanmış ve hizmet sunmaya başlamıştır. Günümüzde ise bu bağlantılar artık dünya nüfusunun yarısından fazlası tarafından kullanılmaktadır. Çünkü internet bağlantısı yapan kişi sayısı her gecen gün artış göstermektedir. Bu durum ise siber saldırıların ve tehditlerin artmasına neden olmaktadır. Siber alan içerisinde sağladığı imkanlar dahilinde sadece devletler kullanmaz. Birçok terör grupları tarafından da aktif olarak kullanılmaya başlanmıştır. Siber alanda oluşturulan kötü yazılımlar hedef gösterilen sistemin çalışmasını engel olmayı amaç edinmiştir. Bu sayede gizli tutulan bilgileri bulmak hedeflenmiştir

Devletler veya devlet dışı aktörler sıklıkla teknolojik imkanlardan faydalanmaktadırlar. Yeni nesil bilgi edinme metotlarına başvuru yapan devletler siber uzaydan fazlasıyla etkilenmiştir. ABD, RF, Çin gibi devletlerin yanında devlet dışı aktörler olarak NATO, AB, BM gibi kurumlar da kendi stratejilerini bu alanda geliştirmişlerdir. Devlet dışı kurumlar, siber alanda kendilerini güvenlik açısından geliştirme amacı içerisindedirler.

Siber alan diğer savaş alanlarına göre daha cezbedicidir. Çünkü internet kullanımının maliyetinin düşük olması ve uluslararası etki yaratabilmesi kişiler tarafından cezbedici bulunmuştur. Etkinin büyük yıkımlar yaratabilmesi, medyada yankı bulması, psikolojik haz ve istek uyandırması siber alanı önemli bir savaş alanı haline getirmiştir. Siber alanda yapılan bir saldırının bulunması çok zordur. Çünkü karmaşık bir yapı ve sınırı bulunmuyor. Bu karmaşık

yapı devletler tarafından hoş karşılanmamıştır. Sahip oldukları güvenlik anlayışlarının tehlike altına girebilmesi gibi endişeleri her geçen gün artmaktadır.

Bu duruma en güzel örnek 11 Eylül saldırıları örnek verilebilir. Bu saldırıda siber alanın devlet veya devlet dışı aktörler için mesafelerinin artık olmadığı acı bir gerçek ile yüzleşilmesini sağlamıştır. Böyle bir ortamda internetin önemi anlaşılmış ve siber alanın ne kadar tehlikeli bir savaş alanı olacağını göstermiştir. Bu sayede siber uzay birinci öncelik olmuştur. Çünkü siber alanda artık teknik, politik yasal ve yasal olmayan idari birçok konu siber alan dahilinde incelenmeye başlanmıştır. Siber alanın sağlamış olduğu olanaklar ve bağımlılık her geçen gün artması doğru süreçlerin uygulanması konusunda sıkıntılar yaşatmıştır. Bundan dolayı uluslararası ilişkilerde siber güvenlik konusunu geliştirilmesi en önemli konuların başında gelmektedir.

Siber alanın konusu veya tehdit türlerinin yapısı değiştirilerek devletin almış oldukları stratejileri ve güvenlik konseptlerini buna göre şekillendirecektir. Çünkü devletler bu olaylara ve gelişmelere karşı kendi önlemini almalıdır. Burada İHA ve SİHA alanında alınmayacak güvenlik tedbirleri uluslararası ilişkiler açısından ciddi sorunlar oluşturabilir. İHA ve SİHA alanında yapılabilecek bir saldırı savaşın başlamasına dünya düzenin değişmesine kadar birçok sürecin başlamasına neden olabilir. Devletler, bu olaylara ve gelişmelere karşı kendi önlemini almalıdır. Devlet, uluslararası ilişkilerde dış politikada özellikle kendi varlığın devamını sağlamak istemektedir. Uluslararası sistemin sağladığı kurallar içerisinde devletler, çıkar ve güç mücadelesi içerisinde kaosa sürüklemektedir. Uluslararası ilişkilerde devletler kaos ortamında önem vermesi gereken birçok alan vardır. Siber uzay bunlardan biridir. O yüzden İHA ve SİHA teknolojilerinin gelişmesi uzun vadeli devlet politikaları ve katkıları ile desteklenmelidir. Uluslararası ilişkilerde bu alanların uzmanlıkları sağlanmalı ve yatırımlar yapılmalıdır. Devletler yatırımlar sayesinde stratejiler oluşturulmalıdır.

İnsanoğlu uçabilen nesnelere karşı hep meraklı olmuştur. 1. Dünya Savaşı'nda özellikle uçak üzerine çeşitli araştırmalar yapılmıştır. Savaşta daha az maliyet ile kayıpların az olduğu yüksek teknolojik araçları bulmayı amaç edilmiştir. Bununla birlikte ilk İHA örnekleri ortaya çıkmıştır. Savaşlarda insanlar bilgilerini ve teknolojilerinin zaman içerisinde artmasıyla yeni silahlar keşfetmişlerdir. Her teknolojik yenilikte özellikle savaşta devletler kendi güvenlik algılarını değiştirmeye ve güçlendirmeyi amaç edinmiştir.

Teknolojinin gelişmesi ile birlikte İHA'ların farklı çeşitleri görülmüştür. Başka hava araçlarının da çıkmasıyla birlikte uydu görevi görme potansiyellerine sahip en yüksek aday İHA'lar olmuştur. Günümüzde kullandığımız uydulara göre İHA'ların maliyetleri daha düşüktür. İnsan faktörünün burada daha az kullanılmasıyla birlikte uydunun ilk alternatifi İHA'lar olmuştur. Sadece uydu olarak değil askeri, siyasi, sağlık, istihbarat, telekomünikasyon, enerji, gibi alanların birçoğunda İHA ve SİHA kullanılabilir. Uluslararası ilişkiler açısından devletlerin İHA ve SİHA teknolojilerini aktif kullanması sonradan bazı sorunlara yol açabilir ve birçok felaketi de beraberinde getirebilir. İHA ve SİHA araçlarına siber alan sayesinde müdahalede bulunan

devletler buradaki bilgileri ele geçirebilir veya değiştirebilir. Elde edilen bilgileri sonrasında diğer devletlere karşı kullanabilirler. Bu bilgiler ile ülkeler arasında yeni bir savaşın çıkmasına neden olabilir. Bu yüzden ülkeler açısından çok önemlidir. Bu yüzden gelecek yıllarda İHA ve SİHA hem sivil hayatımızda olsun hem de askeri alanlarda olsun daha geniş alanlarda adını duyuracaktır.

Siber uzayda devletler tehlike altında olmamak için şeffaflık adı altında hareket etmelidir. Lakin ülkeler yürütmüş oldukları İHA ve SİHA gibi sistemleri gizlilik ile saklamakta diğer devletlere karşı kaygı ve korku uyandırmaktadır. Bu gizli ve saklı yapılan gelişmeler uluslararası ilişkilerde devletler için güvensizlik ortamı oluşturmaktadır. Bu ortamda devletler silah kapasitesini artırmaktadır. İnsanlık için tehlikeli olabilecek siber silahlar geliştirmektedirler. Uluslararası ilişkiler açısından baktığımızda İHA ve SİHA alanında güçlenen devletler diğer devletlere karşı bir tehlike oluştururken bu tehlikeyi yenmek için silahlanma yarışına giren devletler uluslararası ilişkiler açısından daha büyük bir tehlike oluşturmaktadır. İHA ve SİHA da elde edilmiş bir bilgi sonrası siber saldırı yöntemiyle değiştirilerek nükleer santrallerde radyasyonu, doğalgaz sızıntılarını, elektrikli tüm sistemlerin çökmesine, uyduların yer değiştirilmesine, silah sistemlerin devre dışı kalmasına, elektrik santrallerde hasarların oluşmasına ve ulusal güvenliğin tehdit altına girmesine sebep olabilir. Bu alanda İHA ve SİHA teknolojilerinin kullanılmasına çok dikkat edilmesi ve siber uzay alanında gerekli tüm önlemlerin alınmasına gerek vardır. Burada başlayacak bir saldırı tüm devletleri etkileyebilir. Uluslararası ilişkiler açısından geri dönülmez zararlar bırakabilir.

Gelişen teknoloji ile birlikte dünya artık birbirine daha fazla bağlı. Artan siber saldırılar ve tehditler sonucunda devletlerin kendi ulusal siber güvenlik stratejilerini oluşturmaya yönelmiştir. Sosyal, siyasi, sağlık, teknolojik gibi faaliyetlerin içerisinde siber uzaya daha çok yer vermesi ile etkileşimin artmasına neden olmuştur. Siber alanın günlük yaşantımıza daha çok yer edinmesiyle güvenlik soruları artmaya başlamıştır. Bu değişimi benimsemeyen kurumlar, siber riski her geçen gün daha fazla hissetmektedirler. Kendi stratejilerini ve yapılarını buna göre dizayn eden devletler ise kendileri daha güvende hissetmektedirler.

Sonuç olarak siber alan günümüze baktığımızda şirketlerin uluslararası ve örgütlerin devletlere kadar geniş bir alanı etkileyen ciddi bir konudur. Siber suç, siber tehdit gibi her yapıyı kişiyi veya kişileri etkileyecek ciddi sorunlar oluştururken küresel birçok felaketin başlangıcı olabilir. Devletler açısından baktığımızda siber alanda sorun yaşamamız için güvenlik önlemlerinin alınması ve siber alanda güvenlik sistemlerinin oluşması gerekmektedir. Bunu kendi için sağlamayan devletler güvenliklerine tam anlamıyla elde etmesi mümkün değildir. Şu an bunu sağlamada İHA ve SİHA gibi teknolojilerden yararlanılmaktadır. Dünyamız artık bu dijitalleşmenin içerisindedir. Uluslararası ilişkilerde siber güvenlik devletler için kaçınılmaz bir alandır, bu yüzden devletler için gerekli önlemleri almayı zorunlu hale getirmiştir. Sadece devletlerin değil şiddet eğilimi gösteren devlet dışı aktörlerin, terör gruplarında insansız silah teknolojisi ile İHA ve SİHA ya sahip olduğu görülmüştür.

Önümüzdeki yıllarda yapılacak yatırımları da düşündüğümüzde İHA ve SİHA gibi teknolojik araçların konvansiyonel sistemlerden daha çok kullanılacağı gerçektir. Bu gerçekliğe önemli bir örnek olarak ABD, Afganistan için yaptığı operasyonlarda SİHA'ları diğer konvansiyonel silahlara göre saldırılarda daha fazla kullanılmasıdır. Sonuç olarak artık muharebe alanları değişmiştir. Burada kullanılan askeri teçhizat ve araçlarda değişikliğe gidilmiştir. Bu değişikliği en önemli yapı taşını İHA ve SİHA sistemlerin oluşturduğunu söyleyebiliriz.

Uluslararası ilişkilerde, İHA ve SİHA teknolojisini sağlayacağı faydalar devletler tarafından bilinmektedir. İHA ve SİHA artık devletler tarafından kabul edilmiştir. Teknolojik gelişmelerini İHA ve SİHA üzerine geliştiren ülkeler önümüzdeki yıllarda askeri olarak diğer devletlerin önünde olacağı açıktır. İHA ve SİHA tarafından gelebilecek bir siber saldırı devletler açısından geri dönülmez birçok zararın oluşmasına da sebep olabilir. Bu tarz sistemlerde saldırı olma ihtimaline karşı bilgisayar ve iletişim alanlarında yerli teknolojilere sahip olunmalı ve devlet tarafından desteklenmelidir. Siber alanda İHA ve SİHA üzerine gelebilecek saldırı, ancak devletlere sahip olduğu teknoloji ve bilgilerin sağladığı misillemeler ile yapılabilmektedir. Siber alanında yaşanılan bu değişimler sadece devletleri değil kuruluşlarında geleneksel güvenlik anlayışından modern güvenlik anlayışına geçmesine sebep olmuştur. İHA ve SİHA üzerinden bir devlete yapılacak saldırı tüm ülkeleri tehdit altına girmesine sebep olur. Örneğin NATO üyesi olan Türkiye'nin, İHA ve SİHA üzerinden bir siber saldırıya maruz kalması gündelik hayatta birçok aksaklıkların oluşmasına sebep olur. Bu yüzden Siber saldırılar sonrasında uluslararası çatışmalara dönüşebilir. Siber alanda İHA ve SİHA üzerinden gelebilecek bir saldırı reel dünyada devletlere vereceği zararların tahminin çok ötesindedir.

İHA ve SİHA'lar günümüzde terör gruplarını yok edilmesi ve vatan güvenliği sağlanması noktasına sıklıkla kullanılmaktadır. Bu otonom araçlarının kullanımı uluslararası ilişkilerde devletler için vazgeçilmez olacaktır. Şu an bunun farkına varmış olan ABD, Türkiye, RF, İngiltere, Fransa, Çin gibi devletler uluslararası ilişkiler açısından güvenliklerini sağlama konusunda bir adım öndedir. İHA ve SİHA konusunda kendilerini geliştirmiş olan bu devletler diğer devletlere karşı bir saldırı durumunda bulunması konusunda endişeler her zaman olacaktır.

İlerleyen zamanlarda SİHA ve İHA'ların kullanılmasında artış olması beklenen bir durumdur. Teknolojini gelişmesi ile daha farklı alanlarda devletler tarafından kullanılacaktır. Bu duruma Türkiye tarafından Deniz Kuvvetleri'ne teslim edilen TCG Anadolu gemisini örnek verilebilir. Bu gemi dünya üzerindeki ilk SİHA gemisidir. Uçuş güvertesinde 10 helikopter, 11 SİHA taşıyabiliyorken 19 helikopter veya 30 SİHA'ya da hangarında bulundurma özelliğine sahiptir. İHA ve SİHA tarihini değiştiren bu gemi yakın zamanda diğer devletler içinde vazgeçilmez olacaktır. Bilgi birikimi artıkça bu tarz gelişmeler ve değişimler İHA ve SİHA kullanımı artıracak ve devletler bu alanda kendilerini geliştirmeye devam edecektir. Sadece savaş zamanında değil barış zamanında sürekliliğin sağlanması konusunda destek olacaktır. Zayiatı en aza indiren

hem de çatışmalar hem de barış dönemlerinde destek sağlayan bu silahların önemsenmemesi mümkün değildir.

Teknolojik ürünlerin askeri alanda daha fazla yer almasıyla birlikte muharebe alanları değişmeye başlamıştır. Özellikle değişen bu alanlarda artık ağ bağlantıları ile düşman unsurları dinlenebilmekte, izlenebilmekte hatta karşı karşıya gelmeden bir tuş yardımı ile müdahale edilebilmektedir. Bu değişimlerden önemli bir kısmını İHA ve SİHA teknolojisi oluşturmaktadır. Özellikle ülkeler, İHA ve SİHA üzerinden yapılan değişiklikleri yakından izlemektedirler. Yaşanılan bu değişimlere karşı kayıtsız kalmayı tercih eden devletler gelecek yıllarda ciddi tehditler yaşayacaklardır. İlk ortaya çıktığında askeri alanda kullanılmaya başlansa da artık sivil hayatta dahi çok aktif şekilde kullanılmaktadır. Bu yüzden yakın zamanda birçok alanda İHA ve SİHA kullanımında artış olacaktır.

Savaş alanlarında yaşanılan değişmeler bu alanlarda kullanılan askeri araçların da farklılaşmasına neden olmuştur. İHA ve SİHA sistemlerinin askeri alanlarda artık daha aktif kullanılması bu duruma örnektir. Yakıt maliyetlerinin düşük olması, içinde pilot olmaması İHA ve SİHA araçlarının kullanılmasında avantaj sağlamıştır. Fiyatının diğer hava araçlarına göre ucuz ve görüntü aktarma kabiliyetinin olması sağladığı diğer avantajlardır. Her ne kadar bu araçlar aktif kullanılıp birçok avantaj sağlamış olsa da bazı olumsuzlukları kendi içerisinde barındırmaktadır.

İHA ve SİHA araçlarının siber uzay, askeri, sağlık gibi farklı alanlarda aktif kullanılması devletlerin saldırıya uğrama riskini artırabilir. Bu durumun yaşanmaması için öncelikle devletlerin ortak bir kararda birleşip açıklama yapmalar gerekir. Çünkü hem siber alanın hem de İHA ve SİHA kullanımın statüsü, hukuki boyutu gibi birçok alanları belirlenmelidir. İHA ve SİHA kullanımın devletlerin sınırlarında kullanılması, hava sahası ihlalleri gibi birçok alanda ortak bir deklarasyon yayınlamalıdırlar. Bu sayede siber alanda gelebilecek saldırılara karşı kendilerini koruyabilirler. Ortak bir karar alınamaması durumunda ise devletler kendi İHA ve SİHA'ların korumalı, elektronik saldırılara karşı önlem almalıdırlar.

İHA ve SİHA'nın bu dönemde sağladığı yararlar göz ardı edilemez. Çatışma içerisinde bu araçların tamamen insansızdan arındığını söylemek doğru değildir. İHA ve SİHA içerisinde kontrolü sağlayan bir insan olmasa da sistemleri oluşturan ve komuta merkezinde kontrol edilmesini sağlayan yine insandır. Komuta merkezlerine gönderilen görüntünün değerlendirilmesi ve hedef unsurlarını yok edilmesi aşamalarında insan figürüne ihtiyaç vardır. Hedefin suçlu veya terörist olup olmadığına karar verme yetkisi insandadır. Bu yüzden insan belirleyici bir rol üstlenmektedir. İHA ve SİHA gibi araçların sadece hedefi yok etme özelliği vardır. İHA ve SİHA'da duygusal zeka özelliği bulunmadığından bazı noktalarda askeri personele ihtiyaç duyulmaktadır. Bu yüzden tamamen insandan arındırılmış, robotların savaşı demek doğru olmaz. Günümüz için bunu söylemek henüz erkendir. İlerleyen zamanlarda teknolojinin daha çok kullanılmasıyla bu durum değişebilir.

KAYNAKÇA

Ak, T. (2018, 04 27). Silahlı İnsansız Hava Araçlarının Kullanımında Karar Mekanizmaları. *Güvenlik Bilimleri Dergisi*, pp. 111-130.

Ak, T., & Avaner, T. (2019, 6 11). Silahlı İnsansız Hava Araçlarının Uluslararası Alanda ve İç Güvenlikte Sevk ve İdaresine İlişkin Hukuki Saptamalar. *Savunma Bilimleri Dergsi, Cilt 18 Sayı 36*, pp. 43-66.

Akyürek, S. (2012). *İnsansız Hava Araçları Muharebe Alanında ve Terörle Mücadelede Devrimsel Dönüşüm(Rapor No:53) .* Ankara: BİLGESAM.

Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları. *İstabul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, Yüksek Lisans Tezi*, 7.

Arslan, Ö. (2021). Türkiye'nin Siber Güvenlik Politikaları ve Siber Saldırılarının Uluslararası Etkileri. *Düzce Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-78.

Atak , V. O., & Aksu, O. (2004). Algılayıcı Yöneltme Sistemleri. *Harita Genel Komutanlığı, Harita Dergisi, Cilt:71 Sayı:132*, 26-37.

Baharçiçek, A., & İnan, C. E. (2013). Dış Politika'nın Belirlenmesinde Ulusal Güvenlik Algısının Rolü. *Akademik Yaklaşımlar Dergisi, 4(1)*, 101-120.

Bakan, S., & Şahin, S. (2018). Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler. *The Journal of International Lingnual, Social and Educational Sciences, 4(2)*, 135-152.

Barış , Ö. (2021). Etkin Siber Güvenlik Stratejilerinde Yönetim Bilişim Sistemlerinin Yaklaşımları. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-102.

Başeskioğlu, M. Ö. (2021). Siber Güvenlik, Bilgisayar Ağları, Kimlik Avı, Kötü Amaçlı Yazılım, Fidye Yazılımı, Sosyal Mühendislik Biçiminde Korsanlıkta Korumaya Yönelik İncelemeler ve Bir Uygulama. *Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi*, 1-135.

Baştürk, R. (2015). Kolluk Kuvvetlerinin İstihbarat Temininde Başvurabileceği İnsansız Hava Araçları(İHA) ve Bu Açıdan Uygun İHA Özelliklerinin Araştırılması. *Harp Akademileri Stratejik Araştırmları Enstitüsü, Yüksek Lisans Tezi*, 1-116.

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat . *Güvenlik Stratejileri, 10(20)*, 119-147.

Bergen, P., Salyk-Virk, M., & Sterman, D. (2020, 07 30). Worl of Drones. Retrieved from New America: https://www.newamerica.org/international-security/reports/world-drones/

Bıçakçı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi, 9(34)*, 205-226.

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik.* İstanbul: 2013.

Bilen, A. (2021). Akıllı Yöntemler ile Siber Saldırı Sisteminin Geliştirilmesi. *Fırat Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi*, 1-90.

Bilgiç, A. (2012). *''Güvenlik İkilemini Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif'', Mustafa Aydın ve diğerleri (Ed), Uluslararası İlişkilerde Çatışmadan Güvenliğe, 1. Baskı içinden (337-352),.* İstanbul: İstanbul Bilgi Üniversitesi.

Birer, G. C. (2022, Mayıs). Silahlı İnsansız Hava Araçları. *Tubitak- Bilim Teknik*, pp. 65-73.

Burgaz, M. (2020). Derin Öğrenme Algoritmaları Kullanarak İnsansız Hava Araçaları ile Sİlah Tespiti. Batman Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 1-108.

Caner, E. (2013). İnsansız Hava Araçları. *Milli Güvenlik ve Askeri Bilimler Akademik Dergisi, Cilt 1 Sayı 1*, 213-240.

Cengiz, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. *İletişim Çalışmaları Dergisi*, 407-424.

Ceylan, C. (2010). *Ağ Merkezli Savaşta, Aviyonik Sistemleri Bulandırma Saldırıları. Erişim tarihi: 18 Şubat 2010*. Retrieved from https://doczz.biz.tr/doc/134958/a%C4%9F-merkezli-sava%C5%9Fta-%20aviyonik-sistemleri

Coşar, M. (2022). Attacks on Unmanned Aerial Vehicles and Cyber Security Measures. The Eurasia Proceedings Of Science, Technology Engineering & Mathematics (EPSTEM) Cilt 21, pp. 258-265.

Çakmak, H., & Altunok, T. (2009). *Suç, Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Yayınevi.

Çaycı, S. (1995). *Silahlı Kuvvetlerin Kullanılması.* Ankara: Genelkurmay Basımevi.

Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Multidisiliner Bir Yaklaşım. *Academic Review of Humanites and Social Sciences, 1(2)*, 110-119.

Çetinkaya, Ş. (2012). Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları. *21. Yüzyılda Sosyal Bilimler, Sayı 2*, 241-260.

Çiftçi, H. (2013). Her Yönüyle Siber Savaş. Ankara: Tubitak Yayınları.

Darıcılı, A. B., & Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG), Avrasy'nın Siyasal Özel Sayısı, 121-146.

Dedeoğlu, B. (2018). *Uluslararası Güvenlik ve Strateji(4. Baskı).* Yeniyüzyıl Yayınları.

Demir, A. (2001). Savaş Sanatı. İstanbul: Kastaş Yayınları.

Düz, S. (2022). *Türkiye'nin S/İHA Endüstrisi Üzerine Tartışmalar.* Ankara: SETA.

Emir, B. (2020). Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi. *Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-137.

Erdağ, R. (2020). Savaş ve Çatışmanın Değişen Yapısı: Sailahların İnsansızlaştırılması. *Güvenlik Çalışmaları Dergisi, Cilt:22 Sayı: 1*, 3-22.

Erdem, M., & Özocak, G. (2019). Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukun Rolü. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 127-212.

Erdem, T. (2020). 21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay. *Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi*, 1-300.

Eren , M. (Mart 2017). *Avrupa Birliği'nin Siber Güvenlik Politikası.* İstanbul: Beta Yayınları.

Girgin, K. (2003). *Uluslararası İlişkiler Modern İstihbarat ve Türkiye.* İstanbul: Okumuş Adam Yayınları.

Gutnıkov, A., Kupreev, O., & Yaroslav, Ş. (2022). 2022'nin İlk Çeyreğinde DDoS Saldırıları Erişim Tarihi: 25.04.2022. Retrieved from Securelist Web Sitesi: https://securelist.com/ddos-attacks-in-q1-2022/106358/

Güleç, Ö. (2021). Uluslararası İlişkilerde Siber Güvenlik Kavramı ve Uygulamaları. *Fırat Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-88.

Güngör , M. (2015, Mart). Ulusal Bilgi Güvenlği: Strateji ve Kurumsal Yapı . *Türkiye Cumhuriyeti Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, Uzmanlık Tezi*, pp. 1-129.

Güntay, V. (2016). Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT). *Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi*, 6-209.

Gürkaynak, M., & İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, C.16, S.2*, 263-279.

Güven, A. S. (2021). Türkiye ile Avrupa Birliği'nin Siber Güvenlik Stratejilerinin Karşılaştırılması. *Muğla Sıtkı Koçman Üniversitesi, Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi*, 1-70.

Hambling, D. (2020). The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia Erişim tarihi: 10.11.2020. Retrieved from Forbes Web Sitesi: https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/?sh=204c48195e57

Hambling, D. (2023). Ukraine Is Spoofing Russian Drones Out Of The Sky Erişim Tarihi: 21.04.2023. Retrieved from Forbes Web Sitesi: https://www.forbes.com/sites/davidhambling/2023/04/21/ukraine-is-spoofing-russian-drones-out-of-the-sky/?sh=636b2078100c

Idan, A. M. (2020). Ulusal ve Uluslararası Güvenliğin Bileşeni Olarak Siber Güvenlik: Irak Örneği. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi*, 1-234.

İrdem, İ., & Bayansar, R. (2022). Özgürlük- Güvenlik İkilemi ve İnsan Hakları Bağlamında Kolluğun Toplumsal Olay Yöntemi. *Sosyal Bilimler Enstitüsü Dergisi*, 140-155.

İşçi, İ., Görmüş, G., Aydoğmuşoğlu, B., & Mekin Pesen, M. (2017). Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır Erişim Tarihi: 22.07.2017. Retrieved from Sibergah Web sitesi: https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/

Jahn, T., Bomke, L., Kroll, H., & Demircan, O. (2022). Hyperschallraketen, Drohnen, Künstliche Intelligenz: Diese Technologien nutzt die Waffenindustrie Erişim Tarihi: 20.06.2022. Retrieved from https://www.handelsblatt.com/technik/ruestungsindustrie-hyperschallraketen-drohnen-kuenstliche-intelligenz-diese-technologien-nutzt-die-waffenindustrie/28427246.html

Kahveci, M., & Can, N. (2017). İnsansız Hava Araçları: Tarihçesi, Tanımı, Dünyada ve Türkiye'deki Yasal Durumu. *Selçuk Üniversitesi Mühendislik, Bilim ve Teknoloji Dergisi, 5(4)*, 511-535.

Karaağaç , C. (2016). İHA Sistemleri Yol Haritası- Geleceğin Hava Kuvvetleri 2016-2050. *STM Mühendislik Danışmanlık, STM*, 1-48.

Karabulut, B. (2015). *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek.* Ankara: Barış Kitabevi.

Karakuş, C. (2019, 01 30). Silahlı İnsansız Hava Araçlarının (SİHA'lar) Konvansiyonel Savaştaki Yeri: Anlık İstihbarattan Anlık Müdahaleye Geçiş. *İstanbul Aydın Üniversitesi, Yüksek Lisans Tezi*, pp. 1-140.

Katrancı, S. (2020). İnsansız Hava Aracı (İHA) ve Silahlı İnsansız Hava Araçlarının (SİHA), Hibrit Savaşta Kullanımı ve Türk Silahlı Kuvvetleri'ne Etkisi. *Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-117.

Korkmaz , Y., İyibilgin, O., & Fındık, F. (2016). Geçmişten Günümüze İnsansız Hava Araçlarının Gelişimi. *Sakarya Üniversitesi Fen Bilimleri Dergisi, Cilt 20, Sayı 2*, 103-109.

Korkusuz, A. (2020). Kurumlarda Siber Güvenlik ve Siber Riskler. *Bahçeşehir Üniversitesi. Yüksek Lisans Tezi*, 1-91.

Kotik, Y. Ö. (2015). Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişen Stratejisi. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-96.

Küçük, G. (2022). Siyasal Pazarlama Bağlamında, 2020 Karabağ Savaşında İHA ve SİHA'ların Önemi. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-118.

Lendon, B. (2023). Three weapons that changed the course of Ukraine’s war with Russia Erişim Tarihi: 25.02.2023. Retrieved from Edition CNN Web sitesi: https://edition.cnn.com/2023/02/25/europe/ukraine-war-three-key-weapons-intl-hnk/index.html?utm_content=2023-02-26T09%3A15%3A07&utm_medium=social&utm_term=link&utm_source=twCNNi

Malsin, J., & Kıvılcım, E. (2022, Temmuz 21). *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/drones-unmanned-boats-and-killer-robots-have-made-turkey-an-arms-industry-powerhouse-11658404887?mod=Searchresults_pos5&page=1

Mevlütoğlu, M. A. (2018). Geleceğin Savaşları.Erişim tarihi: 10.06.2018. STM Mühendislik Teknoloji Danışmanlık. Retrieved from STM Mühendislik Teknoloji Danışmanlık: https://www.stm.com.tr/documents/file/Pdf/10.Gelece%C4%9Fin%20Sava%C5%9Flar%C4%B1_2016-08-03-11-01-18.pdf9.

Mutlu Genç, Y., & Erciyes, E. (2020). İnsansız Hava Araçları (İHA) Tehditleri ve Güvenlik Yöntemi. *Türkiye İnsansız Hava Araçları Dergisi*, 36-42.

Nişancı, M. H., Teşneli, A. Y., & Teşneli , N. B. (2018, 09 11). Yıldırım Darbelerinin Silahlı İnsansız Hava Araçları (SİHA) Üzerindeki Dolaylı Etkilerinin Analizi. *Sakarya Üniversitesi Mühendislik Fakültesi Elektrik Elektronik Mühendisliği Bölümü, Mühendislik Bilimleri ve Tasarım Dergisi 6(3)*, pp. 390-395.

Ok, M. (2015). Soğuk Savaş Sonrası NATO'nun İcra Ettiği Askeri Müdahalelerin Türkiye Perspektifinden İncelenmesi. *İzmir Katip Çelebi Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Ana Bilim Dalı, Yüksek Lisans Tezi*, 1-204.

Özcan, A. B. (2011). Uluslararası Güvenlik Sorunları ve ABD'nin Güvenlik Stratejileri. *Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Sosyal ve Ekonomik Araştırmlar Dergisi, Sayı 22*, 446-462.

Özcan, M. (2014). Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu Erişim tarihi: 17.02.2014. Retrieved from BookReader Web Sitesi: http://bookre.org/reader?file=1183626&pg=2

Özçoban, C. (2014). 21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü. *Harp Akademileri Stratejik Araştırmaları Enstitüsü, Yüksek Lisans Tezi*, 1-101.

Özerdem, A. (2021). SİHA'ların Kullanımında Etik Boyut. *Liberal Düşünce Dergisi, Sayı: 104*, 145-162.

Özfındık, Ö. (2021). İnsansız Hava Araçlarının Adli Bilişim Açısından İncelenmesi . *Güvenlik Bilimler Dergisi, Kasım, Cilt: 10 Sayı : 2*, 425-446.

Payam, M. M. (2018). Emniyet, Güvenlik, Kent Emniyeti ve Kent Güvenliği : Kavramsal Bir Analiz. *Eurasscience Journals Avrasya Terim Dergisi 6(1)*, 15-25.

Peker, A. (2013). İnsani Değerler Yönelimli Psiko-Eğitim Programının Problemli İnternet Kullanımı ve Siber Zorbalık Üzerinden Etkisi. *Sakarya Üniversitesi, Eğitim Bilimleri Enstitüsü,Doktora Tezi*, 1-225.

Sandilaç, N. (2021). Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları, . *Sakarya Üniversitesi, Yüksek Lisans Tezi*, 1-100.

Sökmen, E. Ç. (2022). iHA ile Olay Yeri İnceleme ve Dokümantasyon. *Polis Akademisi Adli Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-119.

SSM. (2017). Savunma Sanayi Müsteşarlığı, Türkiye İHA Sistemleri Yol Haritası 2011-2030 Erişim Tarihi: 23.10.2017. Retrieved from SSM Sitesi: http://www.ssm.gov.tr/_layouts/images/iha_ekatalog_web/files/assets/seo/to c.html

Suscan, A. (2022). Türkiye'nin Terörle Mücadele Harekatında IHA/ SİHA Kullanımının Etkisinin Analizi. *Kapadokya Üniversitesi Lisansüstü Eğitim, Öğretim ve Araştırma Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi*, 1-186.

Sütçüoğlu, Ö., & Alay, M. (2019). *Anti-Drone Savunma Sistemleri.* Ankara: STM Teknoloji Düşünce Merkezi.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl. *Uluslararası Bilgi Güvenlği Mühendisliği Dergisi, 2 (2)*, 10-17.

Tanrıverdi, M. (2014). İstanbul: ASSAM.

Tarhan, K. (2018). Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik. *Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-88.

Tekerek, M. (2008, 06 30). Bilgi Güvenliği Yöntemi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Fakültesi*, pp. 132-137.

Terkan, A. (2015, 05 30). Terörizmle Mücadele Kapsamında İnsansız Hava Araçlarının Rolü: Fedaral Yönetimli Aşiret Bölgesi Örneği. *Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yüksek Lisans Tezi. Ankara*, 1-195.

Topal, A., Akpınar, M., & Beyhan, H. (2021). Hale Sınıfı İnsansız Hava Aracı Teknolojisi ve Konvansiyonel (Geleneksel) Savaştaki Yeri. *Türkiye İnsansız Hava Araçları Dergisi, 3(1)*, 17-22.

Trofimov, Y., & Nissenbaum, D. (2022). Russia's Use of Iranian Kamikaze Drones Creates New Dangers for Ukrainian Troops Erişim tarihi: 17.09.2022. Retrieved from ttps://www.wsj.com/articles/russias-use-of-iranian-kamikaze-drones-creates-new-dangers-for-ukrainian-troops-11663415140?mod=Searchresults_pos6&page=1

Ulutaş, G. (2018). *Siber Güvenlik. Siber Güvenlik ve Savunma: Farkındalık ve Caydırma.* Ankara: Grafiker.

Ünal , S. (2015). Siber Uzamın Güvenlikleştirme Söylemi : Türkiye, ABD ve Avrupa Birliği Örnekleri. *Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi*, 1-377.

Ünsal , Ş. (2010). Milli Güç, Bileşenleri ve Vasıtları. *Türk Dünyası Araştırmaları, Sayı : 187*, 27-50.

Yalçın, N. O., & Boyacı, A. (2020, 05 31). İnsansız Hava Araçlarının Hareket ve Yönlendirme Protokellerine Göre Performans Ölçümü. *Teknoloji ve Uygulamalı Bilimler Dergisi Cilt 3, No 1*, pp. 27-40.

Yarman, T. (2011). *Geçmişte ve Bugün Nükleer Enerji Tartışması.* İstanbul: Okan Üniversitesi Yayınları.

Yayla, M. (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. *Hacattepe Hukuk Fakültesi Dergisi. 4(2)*, 181-200.

Yener , Z. (2013). Siber Uzay Güvenliği : Ulusal Güvenlik ve Uluslararası Güvenliğe Etkileri. *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-138.

Yeşiltaş, M., & Duran, B. (2018). *Ortadoğu'da Devlet Dışı Silahlı Aktörler: Terör Örgütleri, Milisler, Vekil Güçler.* İstanbul: SETA Kitapları.

Yıkıcı, İ. (2020). Siber Teknolojilere Dayalı Yeni Uluslararası Güvenlik Konsepti Bağlamında Türkiye Siber Güvenlik Stratejisi. *Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi*, 1-136.

Yılmaz , B. A. (2020). Siber Terörizm ve Değişen İstihbarat Anlayışı . *Anadolu Strateji Dergisi*, 65-81.

Yılmaz, İ., Keiyinci, S., Çam, Ö., & Karcı, A. (2017). Çırpan Kanadın Aerodinamik Parametrelerinin Deneysel Olarak İncelenmesi. *Gazi Üniversitesi Mühendislik Mimarlık Dergisi 32:4*, 1035-1050.

Yılmaz, S., & Salcan, O. (2008). *Siber Uzay'da Güvenlik ve Türkiye.* İstanbul: Milenyum Yayınları.

Yılmaz, Ü. (2019). İnsani Yardım Lojisitiği Faaliyetlerinde İnsansız Hava Araçlarının Kullanım Alanları. *Türkiye Mesleki ve Sosyal Bilimler Dergisi, S.2*, 43-54.

Yorulmaz, M. (2014). ''Değişen'' uluslararası güvenlik algılamaları bağlamında Türkiye-Yunanistan ilişkilerinde ''değişmeyen'' güvenlik paradoksu. *Balkan Araştırma Enstitüsü Dergisi. 3(1)*, 103-135.