



Erzincan Binali Yıldırım Üniversitesi
Hukuk Fakültesi Dergisi
Erzincan Law Review

Cilt/Vol: 29 Sayı/No: 2 Aralık/December 2025

Dış Uzayda Gerçekleştirilen Siber Saldırıların Hukuken Değerlendirilmesi

Legal Assessment of Cyber Attacks in Outer Space

  **Doç. Dr. Merve Ayşegül KULULAR***

 10.60002/ebyuhfd.1683198

ÖZ

Uzay faaliyetleri bilişim teknolojilerindeki gelişmelerden etkilenmiştir. Bu etkileşim yapay zekâ destekli sistemler kullanılarak bilimsel gelişime katkı sunulması şeklinde olabildiği gibi kinetik saldırılara alternatif siber saldırıların gelişerek artması şeklinde de olabilmektedir. Bu bağlamda siber saldırılar Dış Uzay Anlaşması kapsamında benimsenmiş olan uzayın barışçıl kullanımı ilkesi karşısında büyük bir risk teşkil etmektedir. Siber saldırıların düşük maliyetli olması, anonim gerçekleştirilmeye elverişli olması, özellikle yapay zekâ destekli sistemler tarafından algoritmik sorun sonucu mu yoksa kasıtlı olarak mı gerçekleştirildiğinin belirlenmesinin oldukça güç olması siber saldırıların uzay faaliyetlerinde teşkil ettiği sorunlardan bazılarıdır. Ayrıca uyduda gerçekleşen kısa süreli işlevsizliklerin siber saldırı mı yoksa uydudaki sistemsel bir bozukluk mu olduğunun tespitinin hemen hemen imkânsız olması, uydular üzerinde siber saldırı tespit

* Hacettepe Üniversitesi, Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı.

Makale Bilgisi/Article Info: Araştırma Makalesi/Research Article

Geliş/Received: 24.04.2025 | **Kabul/Accepted:** 15.09.2025.

Bu makale, intihal programında taranmış ve iki (kör) hakem incelemesinden geçmiştir. This article was submitted in a plagiarism program and reviewed by two (blind) referees.

Atıf/Cite as: Merve Ayşegül Kulular, “Dış Uzayda Gerçekleştirilen Siber Saldırıların Hukuken Değerlendirilmesi”, EBYÜ-HFD, C. 29, S. 2, Aralık 2025, (817-843).



Bu makale **Atıf-GayriTicari 4.0 Uluslararası** lisansı ile lisanslanmıştır.

edilse dahi bu saldırının hangi amaçla gerçekleştirilmiş olduğunun ve saldırı sonrası hangi zararın doğduğunun belirlenmesi de çok zordur.

Uzayda gerçekleşen siber saldırılara özgü nitelikler dikkate alınarak çalışmada dış uzayda gerçekleştirilen siber saldırıların mevcut anlaşmalar kapsamında analiz edilmesi amaçlanmıştır. Bu bağlamda dış uzayda gerçekleştirilen kinetik saldırıların ve siber saldırıların neler olabileceği incelenmiş, askeri amaçlı uzay faaliyetleri üzerine odaklanılarak astronotun durumu ve hem askeri hem sivil amaçlı kullanılan uyduların durumu ilgili uluslararası anlaşmalar ve insani hukuk kapsamında tartışılmıştır. Devlet yahut devlet dışı aktörler tarafından gerçekleştirilen siber saldırılarda sorumluluğun belirlenerek zararın giderilmesinde hem dış uzayın hem de siber uzayın nitelikleri dikkate alınarak uzayın barışçıl kullanımı için hukuki bir mekanizma oluşturulması gerektiği sonucuna ulaşılmıştır. Bu bağlamda Birleşmiş Milletler bünyesinde bir tür tahkim merkezinin kurulması önerilmektedir.

Anahtar Kelimeler: Dış Uzay Anlaşması, Siber Saldırı, Siber Güvenlik, Yayı Zekâ, Birleşmiş Milletler Tahkim Merkezi.

ABSTRACT

Information Technologies affects space activities. This impact could be seen by AI-implemented developed space technologies. On the other hand, information Technologies have adverse impacts on space activities considering cyber attacks. In this context, cyber attacks pose a great risk to the principle of peaceful use of outer space adopted with the Outer Space Treaty. Low-cost, and anonymity of cyber-attacks could be main phenomena to spread cyber-attacks in outer space. On other words, it is very difficult to determine the reason of the problem on a satellite whether it is a result of algorithmic output or it is a result of an intentional cyber attempt. In addition, it is almost impossible to find out the reason for system failure since the reason might be cyber-attacks including disruptions to a network, or malfunctioning software, or hardware. Even if a cyber attack is detected on satellites, it is very difficult to determine purpose of it. Accordingly it is extremely difficult to determine what the real damage occurred by cyber-attack is.

This study aims to analyze cyber attacks in outer space within the scope of existing international agreements. In this context, it assesses kinetic attacks and different types of cyber attacks in outer space. Considering international agreements of space law and humanitarian law, this work discussess military space activities regarding to their risks, the status of astronauts and the status of dual-use satellites acting for both military and civil purposes. It illustrates the significance of establishing a legal mechanism considering the characteristics of both outer space and cyber space for peaceful use of outer space. The work assess issues on determining responsibility and damages caused by cyber attacks carried out by state or non-state actors. In this context, to cope with issues relavent to

cyber-attacks and to minimise cyber attacks this research proposes a new type of formal arbitration center in the United Nations context.

Keywords: Outer Space Treaty, Cyber Attack, Cybersecurity, Artificial Intelligence, United Nations Arbitration Center.

GİRİŞ

Bilişim teknolojilerinin dış uzayda kullanımı bilim ve teknolojinin gelişiminde ve yeni keşiflerde önemli etkilere sahiptir. Diğer taraftan, siber saldırılar gibi kötü amaçlı kullanımlar uzayın barışçıl amaçlarla kullanımı ilkesini ihlal etmekte ve ayrıca sadece uzayda değil sivil halk üzerinde de önemli zararlara neden olabilmektedir. Özellikle dış uzayda uydular üzerinde gerçekleştirilen saldırı yöntemlerinin bilişim teknolojilerinin etkisiyle artık kinetik saldırı yerine elektronik olarak siber saldırılar kullanılarak gerçekleştiriliyor olması, hukuki açıdan çeşitli sorunlar oluşturmaktadır. Uydular üzerinde gerçekleştirilen kinetik saldırılarda fiziksel olarak uyduya zarar verilmesi gerektiğinden fiziksel olarak verilen bu zararlar iliyet kurulabilecek ülkenin tespit edilmesi ve zararın giderilmesinde hangi ülkenin sorumlu tutulması gerektiği siber saldırılara oranla net olarak belirlenebilmektedir. Ayrıca Dış Uzay Anlaşması gibi taraf devletlerce sorumluluğa dair şartların belirlendiği uygulanagelmekte olan eski tarihli anlaşmalar ve bunlar üzerine yapılan bilimsel araştırmalar neticesinde kinetik saldırılara yönelik sorunlu konuların çözümüne gidilebilmektedir. Örneğin dış uzayda doğan zarara neden olan kinetik saldırının tespiti, saldırının kamu tüzel kişiliği haricinde bir tüzel kişiliğin uydusu tarafından gerçekleştirilmesi durumunda yahut birden fazla devletin kullanımına tahsis edilmiş bir uydu tarafından gerçekleştirilmiş olması gibi tartışmalı konularda kimin sorumlu tutulacağına belirlenmesi gibi konularda uluslararası literatürde tartışmalar ve çözüm önerileri süregelmektedir.

Dış uzayda siber saldırı gerçekleştirilerek yer yüzünde yahut dış uzayda zarara neden olunması halinde ise zarara veya bozukluğa neden olan olayın bir siber saldırı mı olduğunun tespit edilmesi başlı başına bir sorun oluşturmaktadır. Dış uzayda gerçekleştirilen siber saldırılara yönelik olarak konu gerek teknik anlamda gerekse hukuki anlamda oldukça spesifik olduğundan ulusal ve uluslararası literatürde bu alandaki çalışmalar sınırlı kalmaktadır. Mevcut uluslararası anlaşmaların dış uzayda gerçekleştirilen kinetik saldırılara ilişkin olarak dahi uygulanabilirliğinin sınırlı kaldığı ve güncellenmesi gerektiği tartışılmaktadır. Bu nedenle siber saldırıların kendine has doğasından kaynaklı özellikleri de dikkate alınarak dış uzayda gerçekleştirilecek saldırılardaki muhtemel risklerinin tartışılması önem arz etmektedir.

Bu çalışmada dış uzayda gerçekleştirilen saldırılar türlere ayrılarak incelenmiştir. Bunlardan özellikle askeri amaçlı olanların riskleri tartışılmıştır. Bu bağlamda çalışmada uzayda gerçekleştirilen siber saldırıların uluslararası insani hukuk bağlamında Cenevre Sözleşmelerine Ek Protokol ve Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişkin Protokol kapsamında ve Dış Uzay Anlaşması bağlamında analiz edilmesi amaçlanmıştır. Söz konusu analiz sonucunda dış uzayda gerçekleştirilen siber saldırılarda sorumluluğun belirlenmesi için öneriler sunulması hedeflenmiştir.

I. DIŞ UZAYDA GERÇEKLEŞTİRİLEN SALDIRI TÜRLERİ

Devletler dış uzayda diğer devletlerin uzay faaliyetlerini işlevsiz hale getirmeye yönelik eylemlerde bulunabilmektedir. Bu eylemler, kinetik yani fiziksel saldırılar şeklinde doğrudan diğer ülkenin uzaydaki uydusunu etkisiz hale getiren faaliyetler olabildiği gibi daha farklı teknolojik yöntemler şeklinde de olabilmektedir. Bunların başında elektronik savaş teknikleri, yönlendirilmiş enerji silahları ve siber saldırılar gelmektedir¹. Dış Uzay Anlaşması'nın sadece barışçıl amaçlarla kullanılacak bir uzay vizyonunu hedefleyecek şekilde oluşturulmuş barışçıl çerçevesine rağmen, devletlerin uzayı giderek askeri bir faaliyet alanı olarak görmesi, Dış Uzay Anlaşması'nın etkinliğini tehdit etmektedir. Zira devletler özellikle askeri çıkarlarını gözetecek şekilde uygulamalarda bulunarak dış uzayda birçok barışçıl olmayan faaliyeti siber yöntemler kullanarak gizli olarak yürütmektedir. Bu bağlamda dış uzayda gerçekleştirilen saldırıların temel özelliklerinin incelenmesi gerekmektedir.

A. Kinetik Saldırıların Temel Özellikleri

Kinetik saldırılar, uyduların fiziksel olarak imha edilmesi sonucuna yönelmiş faaliyetlerdir. Bu tür saldırılar, mürettebatlı yer istasyonlarına veya insanların bulunduğu yörüngelerdeki uydulara, örneğin düşük Dünya yörüngesindeki (LEO) Uluslararası Uzay İstasyonu'na (ISS) hedeflenirse,

-
- 1 Elektronik savaş yöntemleri, uyduların iletişimini geçici olarak kesintiye uğratmaktadır. Yönlendirilmiş enerji silahları, hedeflenen uydu sistemlerine lazer veya mikrodalga gibi enerji dalgaları göndererek, uydu sistemlerini işlevsiz bırakabilmektedir. Siber saldırılar ise uydu operasyonlarına müdahale etmek veya kontrol sağlamak amacıyla yazılım ve ağ teknolojileri kullanmaktadır. (Chris O'Meara, "Anti-Satellite Weapons and Self-Defence: Law and Limitations", Düz. L. Lindström, D. Giovannelli, K. Podiņš, D. Štruel C. Kwan, 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon), NATO CCDCOE Publications, Tallinn, Estonya, 2024, s. 252- 256). (National Air and Space Intelligence Center (U.S.), Competing in Space, Federal U.S. Documents Collection, 2018, s. 1.)

doğrudan insan hayatı kaybı potansiyeli taşıyan tek karşı uzay eylemlerinden biridir. Stratejik ve Uluslararası Araştırmalar Merkezi'ndeki (CSIS) Havacılık Güvenlik Projesi tarafından düzenlenen Uzay Tehdit Değerlendirmesi Nisan 2023 raporuna göre bugüne kadar hiçbir ülke başka bir ülkenin uydusuna karşı kinetik fiziksel saldırı gerçekleştirmemiş; ancak Amerika Birleşik Devletleri, Rusya, Çin ve Hindistan olmak üzere dört ülke kendi uydularına karşı doğrudan yükselen uydusavar (Anti-satellite weapons-ASAT) silahlarını başarıyla test etmiştir².

Kinetik yani fiziksel saldırılarda saldırının, saldırıyı gerçekleştiren aktöre atfedilmesi siber saldırılara göre oldukça kolaydır. Zira kinetik saldırılar dakikalar içerisinde fark edilebilmekte ve saldırı sonucu doğacak zarara ilişkin önlem veya yaptırımlar kısa sürede devreye girebilmektedir. Diğer taraftan basit bir siber saldırı örneği olarak ortalama bir veri ihlali ele alındığında; bu siber saldırının gerçekleştirildiğinin tespiti kritik sistemler için bile uzun süre gerektirebilecektir. Ayrıca siber saldırılar, tespitten kaçınacak şekilde gerçekleştirilebilmektedir. Uzayda gerçekleştirilen bir siber saldırı, kritik bir anda tetiklenmeden önce hedef sistemlerde yıllarca hareketsiz kalabilecek şekilde tasarlanabilmektedir³.

B. Elektronik Saldırıların ve Siber Saldırıların Temel Özellikleri

Uydu sistemleri internet altyapılarına giderek daha fazla entegre hale geldikçe, internet yönetimini karmaşıklaştıran siber çatışma ve güvenlik sorunları da uzay hukuku kapsamında incelenmesi gereken önemli konular haline gelmiştir⁴.

2 Kari A. **Bingen ve diğerleri**, Space Threat Assessment, Center for Strategic and International Studies (CSIS), Washington DC, 2023, s. 4. Sovyetler Birliği bu teste ek olarak 1960'ların başlarında eş yörengeli kinetik ASAT silahlarını da test etmiştir. (**Bingen ve diğerleri**, s. 4.)

3 James **Pavur**, Ivan **Martinovic**. "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space", Düz. T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky, 2019 11th International Conference on Cyber Conflict: Silent Battle, NATO CCD COE Publications, Tallinn, Estonya, 2019, s. 6.

4 Larry F. **Martinez**, "The Legal and Policy Dimensions of Cyber-Conflict in Outer Space", Düz. Y. Bayraktar, S. Alis, Proceedings for the Second Symposium on Space Economy, Space Law and Space Sciences, İstanbul University Press, İstanbul, 2023, s. 122.

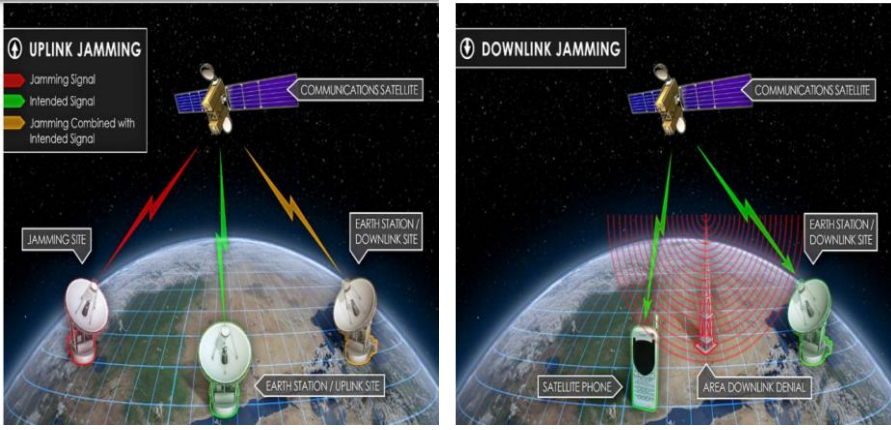
Siber uzay, özellikle ülke güvenliğini tehdit edecek şekilde askeri istihbarata ilişkin olarak gerçekleştirilebilmektedir⁵. Siber saldırılar kullanılarak uydular vasıtasıyla askeri amaçlı istihbarat toplanabilmektedir⁶. Elektronik uydu karşıtı uzay silahları, uzay sistemlerinin veri ilettiği ve aldığı elektromanyetik spektrumu hedef almak üzere kullanılmaktadır. Burada aynı radyo frekansı (RF) bandında gürültü oluşturarak uydulara giden veya uydulardan gelen iletişimlerin engellenmesi amaçlanmaktadır. Bu saldırı faaliyetinde Dünya'dan bir uyduya giden sinyali engellenebilmekte yahut uydudan gelen sinyal Dünya'daki kullanıcılara doğru yayılırken hedef alınabilmektedir. Bu şekilde elektronik saldırılar; bir veri akışına yanlış bilgi enjekte etmek veya bir uydunun işlemlerini bozmak amacıyla uyduya yanlış komutlar vermek için kullanılabilir⁷.

Uydulara gerçekleştirilen siber saldırılara bir diğer örnek ise siber güvenliğin insan unsurlarıyla ilişkili güvenlik açıklarından yararlanarak ağa giriş sağlanması yoluyla. Ağa yapılan bu ilk giriş, saldırganların uydunun güç üretmek, depolamak, kontrol etmek ve dağıtmak için kullanılan elektrik güç sistemindeki güç dağıtım ünitesi için bir aygıt yazılımı güncellemesine gizlice kötü amaçlı kod sokmalarına olanak tanıyacaktı. Bu kötü amaçlı yazılım, pillerde depolanan aşırı enerjiyi -uzay aracının merkezi kontrol sistemini temsil eden veri işleme, komut yürütme ve genel uzay aracı kontrolü gibi kritik işlevleri kolaylaştıran- *komuta ve veri işleme alt sistemine* ve diğer alt sistemlere yönlendirerek bir güç dalgalanması oluşturmaktadır. Bu durum, uydunun iç sıcaklıklarını yükselterek tehlikeli bir durum oluşturmaktadır. Bunun önlenmesi için eş zamanlı olarak saldırganlar tarafından tanıtılan kötü amaçlı yazılım, uydunun içindeki ısıyı düzenlemek için gerekli olan -uzay aracının iç sıcaklığını kontrol ederek görev sırasında sistem bileşenlerini kabul edilebilir aralıklarda tutan- *termal kontrol sistemini* devre dışı bırakmaktadır. Bu şekilde, uydunun tüm alt sistemlerindeki ısıyı düzenleme sistemi bozulmaktadır. Bunun sonucunda güvenlik protokolleri, uyduyu ısıyı azaltmak için alt sistemleri kapatan güvenli bir moda sokacak ve sonunda, yük araçları da dahil olmak

-
- 5 Mustafa Veysel **Güldoğan**/Şevki **Işık**, “Siber Savaşta Mütakabiliyet”, AJIT-e: Academic Journal of Information Technology, S. 51, (Kasım 2022), s. 289, 290, E.T. 03.07.2024.
 - 6 Aybuke İnan **Şimşek**/Senem **Atvur**, “21. Yüzyılda Uluslararası Uzay Rejiminin İnsanlığın Ortak Mirası Temelinde Yeniden İnşası”, Alternatif Politika, C.13, S. 3, 2021, s. 604.
 - 7 **Bingen**, ve diğerleri, s. 5.

üzere elektrik kullanan alt sistemler aralıklı olarak devre dışı bırakılarak etkisiz hale getirilmiş olacaktır⁸.

Karıştırma (jamming) olarak ifade edilen yöntemde ise kullanıcıların hedef sinyali alması engellenmektedir. Uplink sinyal karıştırması uyduya yönelik gerçekleştirilen ve hedef sinyallerle aynı frekansta ve yaklaşık güç seviyesinde çalışması durumunda etkili olabilen bir saldırı çeşididir. Downlink sinyal karıştırması ise işlemin yerdeki kullanıcılara yönelik olarak gerçekleştirilmesinde söz konusu olmaktadır⁹.



Uplink sinyal karıştırması, uyduyu hedef aldığı için etkisi geniş çapta olmaktadır. Zira bu saldırı, uydudan gelen sinyalin, tüm kullanıcılar tarafından alınmasını engelleyebilmektedir. Buna karşılık, downlink sinyal karıştırması sadece yeryüzündeki kullanıcılara yönelik gerçekleştirildiğinden görselde görüldüğü üzere saldırıda kullanılan karıştırıcı cihazın bulunduğu bölgeyle sınırlı bir etkiye sahip olmaktadır.

Siber operasyonların tespit edilmesi zor olduğu gibi tespit edilen bir siber saldırının niçin gerçekleştirilmiş olduğunun tespiti de ayrı bir zorluk taşımaktadır. Bir başka ifadeyle siber saldırıların amacının belirlenmesi oldukça zordur. Nitekim siber saldırılar hedeflenen bir sistemi yok edebileceği veya kalıcı olarak devre dışı bırakabileceği gibi hedef ağdaki özel

8 J. Trenton **Hanan ve diğerleri**, “Analysis of Satellite Systems’ Dependencies and Their Cascading Impacts”, Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2024, s. 495-497.

9 (National Air and Space Intelligence Center (U.S.) 2018, s. 19). Görseller National Air and Space Intelligence Center (U.S.) 2018 s. 18’den alınmıştır.

veya hassas teknik bilgilere erişim sağlamak da dahil olmak üzere casusluk yapmak amacıyla da kullanılabilir¹⁰. Bu durum, uydu davranışlarını anlama ve doğru bir şekilde sınıflandırmayı güçleştirmektedir¹¹. Bir başka ifadeyle dış uzayda gerçekleşen bir faaliyetin kasıtsız bir arıza veya bozukluktan mı ibaret olduğunu yoksa bir siber saldırı olarak mı gerçekleştirilmiş olduğunu tespit etmek oldukça zordur¹². Bunu tespit etmek, gerçekleştirilmiş faaliyetin amacının zarar verme kastını barındırıp barındırmadığının tespiti ile mümkün olacaktır. Bu nedenle gerçekleştirilmiş faaliyetin amacının belirlenmesi, ona göre kasıt var ise faaliyeti gerçekleştiren ülkenin sorumluluğunun belirlenmesinde önemli bir faktördür.

Uzay faaliyetleri bağlamında gerçekleştirilen faaliyetlerde ortada bir uydu karşıtı elektronik saldırı olup olmadığının tespiti sorun teşkil etmektedir. Zira sorun teşkil eden somut olayın bir tür kazara müdahale mi olduğu yoksa bir elektronik saldırı mı olduğunun ayırt edilebilmesi oldukça zordur. Askeri bir hedef oluşturduğu değerlendirilen bir uydunun işlevselliğini devre dışı bırakmak veya bozmak için çok sayıda siber operasyon gerçekleştirilmektedir. Bir başka ifadeyle siber operasyonların geliştirilmesi güncel askeri operasyonlarda önemli bir gerçekliktir¹³. Söz konusu saldırılar şifrelenmiş askerî P(Y) GPS gibi sinyaller üzerinde dahi etkili olarak kullanılabilir¹⁴. Şaşırtma yayım istasyonu (meaconing) gibi elektronik saldırılar; şifrelemenin kırılmasını gerektirmeyip yalnızca orijinal sinyalin zaman gecikmeli bir kopyasını şifresini çözmeden veya verileri değiştirmeden yeniden yayınlamak şeklinde gerçekleştirildiğinden şifreli birçok sinyal üzerinde de uygulanabilmektedir¹⁵. Uzay operasyonları neredeyse tamamen siber bağımlıdır¹⁶. Bir başka ifadeyle uyduların

10 2023'te fırlatılan Rusya'nın ikinci Luch/Olymp uydusunun, muhtemelen istihbarat faaliyetleri yürütmek için jeostasyon yörüngesindeki (GEO) diğer uyduların yakınında konumlandığı düşünülmektedir. (Clayton **Swope ve diğerleri**, Space Threat Assessment 2024, Center for Strategic and International Studies, Washington DC, 2024, s. 4.)

11 **Swope ve diğerleri**, s. 4.

12 Rajeswari Pillai **Rajagopalan**, Electronic and Cyber Warfare in Outer Space, The United Nations Institute for Disarmament Research (UNIDIR), Cenevre, 2019, s. 3.

13 Cassandra **Steer/Dale Stephens**, "International Humanitarian Law and Its Application in Outer Space", War and Peace in Outer Space: Law, Policy, and Ethics içinde, Düz. Cassandra Steer ve Matthew Hersch, Oxford University Press, New York, 2021, s. 50.

14 **Bingen ve diğerleri**, s. 5.

15 **Bingen ve diğerleri**, s. 5.

16 Jana **Robinson**, "Prominent Security Risks Stemming from Space Hybrid Operations", War and Peace in Outer Space: Law, Policy, and Ethics içinde, Düz.

doğası gereği uzay sistemleri neredeyse tamamen siber sistemler kullanılarak işlev sağlamaktadır. Bu tür saldırılarda kullanılan siber teknolojinin, ucuz ve erişilebilir olması hem devlet hem de devlet dışı aktörler arasında siber saldırıların yayılımını kolaylaştırmaktadır¹⁷. Kinetik uydular karşıtı saldırılar için gerekli mali ve teknolojik unsurlar devlet dışı aktörlerin erişiminin ötesinde olduğundan bu tür uydusavar saldırıların devlet dışı aktörler tarafından gerçekleştirilme riski oluşmamakla birlikte saldırıların siber saldırı şeklinde ele alınması durumunda devlet dışı aktörler de devreye girmekte ve bu bağlamda risk önemli ölçüde artmaktadır¹⁸.

Siber saldırılarda temel hedeflerden biri uydulara komuta ve veri dağıtım ağları olup;¹⁹ dış uzayda bunlara yönelik gerçekleştirilen siber saldırılar, yer altyapısını, uzay sistemlerini, kullanıcıları ve bu bölümleri birbirine bağlayan bağlantıları etkilemek üzere gerçekleştirilebilmektedir. Örneğin Çin Halk Kurtuluş Ordusu'nun karasal lazer sistemleri kullanarak ABD görüntüleme uydularını işlevsel kılabilmesinin raporlandığı belirtilmektedir²⁰. Uydular; komuta ve veri ağlarının, güvenlik açıklarına karşı yeterli siber güvenliği haiz olmaması halinde savunmasız kalmakta ve bu nedenle siber tehditler, tüm uydular sisteminin güvenliğini tehlikeye atabilmektedir²¹. Siber saldırılarda kullanılan yöntemlerden biri de uydular yahut

Cassandra Steer ve Matthew Hersch, Oxford University Press, New York, 2021, s. 235.

17 **Bingen, ve diğerleri**, s. 5.

18 Dale **Stephens**/Cassandra **Steer**, "Conflicts in Space: International Humanitarian Law and Its Application to Space Warfare", McGill Annals of Air and Space Law, S. 40, 2015, s. 7.

19 Bu ağlar, uyduların komuta edilmesi (yönetilmesi) ve uydular tarafından elde edilen verilerin dünya üzerindeki merkezlere aktarılması için faydalanılan iletişim sistemleridir. Uydular komuta ağı, uyduların yönlendirilmesi, işlevlerinin kontrol edilmesi gibi yönetim işlevlerini içermektedir. Veri dağıtım ağı ise uydunun topladığı verileri (örneğin; görüntüler, iletişim sinyalleri ya da hava durumu verileri) yer istasyonlarına ulaştırmaktadır. Yer altyapısı temelde uydular ile iletişim sağlayan kontrol istasyonlarını kapsamaktadır. Bu istasyonlar dış uzayda değil dünya üzerinde bulunan istasyonlardır. Ayrıca yer altyapısı kapsamına veri merkezleri de girmektedir. Zira yer altyapısının temel kullanımı; uydunun gönderdiği verilerin işlenmesini ve ardından kullanıcılara iletimini sağlamaya yöneliktir. Uydulara komut göndermek, uydularla haberleşmek ve alınan veriyi işlemek gibi görevler, bu altyapının güvenliği ile doğrudan ilişkili olmaktadır. Uzay sistemleri olarak ifade edilen, yalnızca yörüngedeki uydular değil, uydunun işlevini yerine getirebilmesi için gerekli tüm bileşenleri içermektedir. Bu bileşenlere uydunun kendisi, yörüngedeki diğer destek sistemleri ve uydunun çalışmasını sağlayan yazılımlar da dahil olmaktadır. Uydular hizmetlerinden yararlanan tüm gerçek ya da tüzel kişiler 'kullanıcı' olarak ifade edilmektedir.

20 **Stephens/Steer**, s. 7.

21 National Air and Space Intelligence Center (U.S.), 2018, s. 19.

uzay sistemlerinde normal koşullarda meydana gelen rutin arızaların taklit edilmesidir. Rutin arızalar taklit edilerek gerçekleştirilen siber saldırıların tespit edilmesi oldukça zor olduğu gibi uyduda meydana gelen arızanın gerçekleşmesi muhtemel sıradan bir arıza olmayıp bir siber saldırı olduğu tespit edilse dahi bunun kime atfedilebileceği yani failin ve sorumlunun kim olacağının belirlenmesi de son derece zor bir diğer sorundur.

Uydular üzerinden gerçekleştirilen siber saldırılar “yumuşak öldürme silahları (soft kill weapons)” olarak nitelendirilmektedir²². Yumuşak öldürme ile kastedilen aslında uydunun imha edilmesi değil uydunun fonksiyonlarının işlevsiz hale getirilmesidir. Bu şekilde uyduyu işlevsiz bırakacak saldırılar genellikle gizlice yürütülmektedir. Genellikle uydular üzerinde gerçekleştirilen bir siber saldırının rutin bir arızadan ayırt edilmesi güç olmakta, ayırt edilse dahi siber saldırının kaynağının tek bir tane mi birden fazla mı olduğunun tespit edilmesi, oluşan zararın bu kaynaklara kusur oranlarının paylaşılması zorluk oluşturmaktadır. Yumuşak öldürme silahları kapsamında değerlendirilen havadan lazer testi gibi saldırıların son derece etkili ve hedefe isabetli olarak hassas olduğu bilinmektedir. Bu tür saldırılarda enerjinin konsantrasyonu, kinetik bir saldırının parçalanma etkisine neden olmadan karmaşık devreleri hedef alabilme niteliğini haiz olup bu tür yumuşak silahlar gerçek manada ışık hızında devreye girebilmektedir. Bu tür lazerler uzayda bir yörüngeye konuşlandırılarak saldırı gerçekleştirilebileceği gibi yer tabanlı olarak da konuşlandırılıp yerden uyduya saldırı gerçekleştirilmesinde de kullanılabilir²³.

Yumuşak silahlar kullanılarak gerçekleştirilen siber saldırılar, uydunun imha edilmesine gerek kalmaksızın istenilen süre zarfında uydunun imha edilmişçesine işlevsiz kalmasına neden olduğundan, bunların uydulara saldırı gerçekleştirebilmesi için dış uzayda konuşlandırılma şartı bulunmadığından, yerde konuşlandırılarak da uydunun işlevini etkisiz hale getirme ve bunu ışık hızında ve hassas hedefe ulaşabilecek nitelikte gerçekleştirebilme kapasitesi bulunduğundan kullanımı geleneksel silahlara göre oldukça kolaydır. Uydunun imha edilmesi gerekmediğinden herhangi bir çarpışma gibi imha etmeye yönelik bir metot ile saldırı gerçekleştirmediğinden, uydunun işlevsiz hale getirilmesi uzaktan bir etkiyle sağlandığından bu etkinin kaynağının belirlenmesi ve netice itibarıyla zarardan sorumlunun belirlenmesi oldukça zordur.

22 Stephens/Steer, s. 4.

23 Stephens/Steer, s. 6-7.

Siber saldırıların anonim olarak gerçekleştirilebilmesi hem devlet aktörleri hem de devlet dışı aktörler için uygulanabilir ve düşük maliyetli olması nedeniyle siber saldırıların uzay faaliyetlerinde yaygın olarak kullanıldığı düşünülmektedir. Siber saldırıların haiz olduğu gizlilik ve inkâr edilebilirlik, uzayın barışçıl kullanımını açıkça teşvik eden birçok devletin aynı zamanda gizlice siber uydusavar saldırı yetenekleri (cyber-ASAT) geliştirmelerine imkân sağlamaktadır²⁴.

II. DIŞ UZAYDA GERÇEKLEŞTİRİLEN ASKERİ AMAÇLI SİBER SALDIRILARIN RİSKLERİ

Askeri uçakların navigasyonu için uydu sistemleri, hassas hedefleme ve silah sistemleri; küresel komuta ve kontrol için telekomünikasyon uyduları; füze saldırıları, gözetleme ve keşif için uzaktan sensörler ve diğer uzay tabanlı izleme sistemleri devletlerin silahlı kuvvetleri için kullandıkları uzay sistemlerindendir. Uzayda yer alan uydulara ilişkin olarak devletlerin kullandıkları uzay sistemlerinden bazıları doğrudan ve yalnızca askeri amaçlara özgülenmiş olmakla birlikte birçok sistemin hem sivil hem askeri işlev yürütmekte olduğu savunulmaktadır²⁵.

Uzay sistemlerinin kullanıldığı kritik sivil altyapının işleyişinde yalnızca sivilere iletişim, elektrik gibi temel hizmetlerin sağlanması değil; ayrıca ihtiyaç değerlendirmesinden acil yardım dağıtımına, afet riskinin azaltılmasından uzun süren çatışmalarda sivillerin zarar görmemesine kadar çok çeşitli insani operasyonların sağlanması söz konusudur²⁶. Savaş zamanlarında gıda maddeleri, tarım arazileri, içme suyu tesisleri ve kaynakları ve sulama ağları gibi sivil halkın hayatta kalması için vazgeçilmez olan nesnelere saldırmak, onları yok etmek, kaldırmak veya kullanılamaz hale getirmek yasak olduğu gibi bu nesnelerin üretimi ve bakımı için kritik öneme sahip uzay sistemlerine karşı askeri uzay operasyonlarına ilişkin de aynı yasak geçerlidir²⁷. Ancak bu yasağa rağmen kullanılan silahların giderek daha “güvenilir” olacak şekilde tasarlanmasına önem verilmesine karşın sivil yerleşim yerlerindeki çevresel hasarla ilgili olarak “güvenilirlik” aslında azalmaktadır²⁸. İşleyen kentsel altyapı şebekelerinin çöküşü

24 Pavur/Martinovic, 2019, s. 6.

25 Wen Zhou, “War, Law and Outer Space: Pathways to Reduce the Human Cost of Military Space Operations”, Humanitarian Law & Policy, 15 Ağustos 2023, s. 2.

26 Zhou, 2023, s. 2.

27 Zhou, s. 2.

28 William M. Arkin, “The Environmental Threat of Military Operations”, International Law Studies 69, 1996, s. 126.

paniğe ve işleyen kentsel toplumsal düzenin bozulması korkusuna yol açtığı²⁹ için ‘birini yok etmek için altyapısını yok etmelisiniz’³⁰ anlayışından hareketle uluslararası insani hukuk bağlamında yasak olmasına rağmen devletlerin sivillerin hayatsal fonksiyonlarına ve çevreye zarar verecek şekilde altyapıya kasıtlı olarak zarar verdiği uygulamalarla karşılaşmaktadır. Söz konusu altyapı zararının gerçekleştirilmesinde uzay sistemleri kullanılabilir. Nitekim uydulara ilişkin olarak birçok uzay sistemi askeri işlev yürütmekte olduğu gibi aynı zamanda sivil işlev de yürütmektedir. Uydulara gerçekleştirilecek siber saldırıların özellikle uydu iletişim ve navigasyon sistemleri olmak üzere birçok uzay sistemini sıkıştırıp bozabilecek kapasitede olduğu belirtilmektedir³¹. Diğer taraftan, siber unsurların diğer unsurlara nazaran tercih edilmesi gerektiği, siber unsurlar söz konusu olduğunda insan kaybı riskinin son derece düşük olduğu da savunulabilir³². Hedefe ilişkin fiziksel bir saldırının uygulanması esnası dikkate alındığında bu sav doğru olabilir. Ancak bu durum uydu karşıtı siber saldırıların insanlık için zararsız olduğu algısı oluşturmamalıdır. Zira saldırı tüm süreçleriyle birlikte değerlendirilmeli, saldırı esnasında insanlara yönelik zarar riski düşük olsa da saldırı gerçekleştirildikten sonra uydu işlevsiz hale geleceğinden uydunun insanlara sunduğu kritik hizmetlerin sağlanamaması nedeniyle ortaya çıkacak insani kayıp riski ciddi boyutlarda olabilir. Bir başka ifadeyle uydu karşıtı siber saldırının gerçekleştirilme anında her ne kadar insani kayıp riski düşük olabilse de saldırı gerçekleştirildikten sonra insani kayıp riski önemli boyutlara ulaşabilmektedir.

Savaş sırasında uydulara ilişkin siber saldırıların önlenmesi Dış Uzay Anlaşması kapsamında düzenlenmediğinden uluslararası insancıl hukukun savaş esnasında yapılacak uydu karşıtı siber saldırılara uygulanırlığı analiz edilmelidir.

29 Stephen **Graham**, Switching Cities off Urban Infrastructure and US Air Power, City, C. 9, S. 2, 2005, s. 172.

30 Philip E. **Agre**, Imagining the Next War: Infrastructural Warfare and the Conditions of Democracy, 15 Eylül 2001, s. 1, <https://pages.gseis.ucla.edu/faculty/agre/war.html>, E.T. 01.01.2025.

31 Peter L. **Hays**, “What Should the Space Force Do? Insights from Spacepower Analogies, Doctrine, and Culture”, War and Peace in Outer Space: Law, Policy, and Ethics içinde, Düz. Matthew Hersch, Cassandra Steer, Oxford University Press, New York, 2021, s. 168.

32 **Steer/Stephens**, s. 52.

III. UZAYDA GERÇEKLEŞTİRİLEN SİBER SALDIRILARIN ULUSLARARASI İNSANİ HUKUK BAĞLAMINDA DEĞERLENDİRİLMESİ

Hava muharebeleri savaş hukukunun en tartışmalı alanlarından biridir³³. Uluslararası insani hukuk bağlamında askeri astronotların vatandaşı oldukları ülkelerin savaşa girmesi durumunda hukuki statüleri sivil olarak değil, savaşçı olarak kabul edilecektir. Ancak uzay hukuku dikkate alındığında ise astronotlar “insanlık elçisi” şeklinde değerlendirilmekte ve her zaman koruma, yardım ve destek alma garantisi altında bulunmaktadır. Burada hangi hukukun öncelikli uygulanması gerektiği önem arz etmektedir. Doktrinde askeri personelin devletin silahlı çatışmaya girmiş olduğu esnada astronot olarak görev yaptığı; ancak askeri personel olan astronotun kendisinin savaş eylemlerine katılmadığı durumlarda, hukuki niteliğinin “insanlık elçisi” statüsünde değerlendirilmesi gerektiği belirtilmektedir³⁴. Bu değerlendirmede askeri personel niteliğini haiz astronotun insanlık elçisi olarak ele alınarak koruma altında olmasının sağlanması; devletin savaşta olduğu esnada savaş eylemine katılmaması şartına bağlanmıştır. Benzer değerlendirme uydu karşıtı faaliyetin savaş esnasında gösterilmesi konusunda ele alındığında, uydusavar saldırıyı gerçekleştiren yahut başka bir siber saldırı gerçekleştiren astronotun koruma, yardım ve destek alma garantisinin bulunmadığı sonucuna ulaşılabacaktır. Zira uydusavar saldırı eyleminde bulunan yahut başka bir tür siber saldırı gerçekleştiren astronot “insanlık elçisi” niteliğini haiz olmak için gerekli olan savaş eyleminde bulunmama şartını karşılamadığından insanlık elçileri için getirilmiş olan korumadan da faydalanamayacaktır.

Birinci Dünya Savaşı’nda uçakların yalnızca keşif için değil, aynı zamanda kendi başlarına, özellikle düşmanın cephenin çok gerisinde kalan ve kara veya deniz kuvvetlerinin erişemediği yerleşim ve sanayi bölgelerine saldırmak için silahlar olarak çok daha etkili bir şekilde kullanılabileceğini göstermesi³⁵; hava ve uzay sahasına ilişkin düzenlemelerin sivillerin korunmasındaki gerekliliğini ortaya koymuştur. 8 Haziran 1977 tarihli “12 Ağustos 1949 tarihli Cenevre Sözleşmelerine Ek Protokol ve Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişkin Protokol

33 Heinz Marcus **Hanke**, The “1923 Hague Rules of Air Warfare — A Contribution to the Development of International Law Protecting Civilians from Air Attack”, International Review of the Red Cross Cambridge University Press, C. 33, S. 292, 2010, s. 12.

34 **Stephens/Steer**, s. 15.

35 **Hanke**, s. 13.

(Protokol I)'''de düzenlenmiş olan 52. maddede sivil nesnelerin saldırı veya misilleme nesnesi olamayacağı hüküm altına alınmıştır. 52. madde-nin 2. fıkrasında ise,

“Saldırıları kesinlikle askeri hedeflerle sınırlıdır. Nesneler söz konusu olduğunda, askeri hedefler, doğası, konumu, amacı veya kullanımı itibarıyla askeri eyleme etkili bir katkıda bulunan ve o sırada geçerli olan koşullar altında tamamen veya kısmen imha edilmesi, ele geçirilmesi veya etkisiz hale getirilmesi kesin bir askeri avantaj sağlayan nesnelerle sınırlıdır.”³⁶

şeklinde belirtilerek savaş sırasında dahi sivil unsurların korunması amaçlanmıştır³⁷. Bu madde bağlamında askeri hedefin ne olduğu değerlendirilirken taşınması gereken unsurlar belirtilmiştir. Buna göre söz konusu hedef; askeri eyleme etkili bir katkı sağlayacak olmalı ve bu katkı söz konusu hedefin doğası, konumu, amacı veya kullanımı sayesinde olmalıdır. Ayrıca hedefin tamamen veya kısmen imhası, ele geçirilmesi veya etkisiz hale getirilmesi, o anki koşullar altında belirgin bir askeri üstünlük sağlamalıdır³⁸.

12 Ağustos 1949 tarihli Cenevre Sözleşmelerine Ek Protokol ve Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişkin Protokol (Protokol I)'in 52. maddesi 2. fıkrası uyarınca bir uydunun askeri hedef olabilmesi için *“doğası, konumu, amacı veya kullanımı itibarıyla askeri eyleme katkı sunuyor”* olması şartı bulunmaktadır. Uyduya yapılan saldırının askeri hedefe yapılmış olarak değerlendirilebilmesi için uydunun belirli bir askeri şekilde kullanımının amaçlandığı düşüncesinin temellendirilebileceği yeterli istihbarat ve bilgi olmalıdır³⁹.

Bir başka ifadeyle bir uydunun konumlandırıldığı yerin askeri amaçlı kullanıma elverişli olduğunun düşünülmesi yahut uydunun askeri amaçlı

36 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), International Humanitarian Law Databases, International Committee of the Red Cross, 8 Haziran 1977.

37 Protokol'ün ‘Sivil Halkın Hayatta Kalması İçin Vazgeçilmez Olan Nesnelerin Korunması’ başlıklı 54. maddesinde ise sivilleri aç bırakmak, onları göç ettirmek veya başka bir amaç gibi her ne amaçla olursa olsun sivil halkın yaşaması için vazgeçilmez olan gıda maddeleri, gıda maddeleri üretimi için kullanılan tarım alanları, mahsuller, hayvanlar, içme suyu tesisleri ve kaynakları ve sulama tesisleri gibi nesnelere saldırmak, bunları yok etmek, kaldırmak veya işe yaramaz hale getirmek yasaklanmıştır. (Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1977).

38 Stephens /Steer, s. 17.

39 Stephens /Steer, s. 17-18.

kullanım potansiyelinin bulunması gibi durumlar nedeniyle hedef alınması durumunda Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişkin Protokol'ün 52. maddesi 2. fıkrası ihlal edilmiş olacaktır. Zira bu fıkra uyarınca bir uyduya saldırı gerçekleştirilebilmesi için uydunun askeri hedef olması şartı bulunmaktadır. Askeri hedef olarak nitelendirilebilmesi için ise uydunun gelecekte bir muhtemel askeri amaçlı kullanım tehlikesinin bulunması yeterli değildir.

Uluslararası insani hukukun temel ilkelerinden olan savaşa olan muharipler ile siviller arasındaki ayrım ilkesinin hem sivil hem askeri işlev yürüten çift işlevli uydular açısından etkili bir ilke olma özelliğini yitirdiği değerlendirilebilir. Savaşa olan muharipler ile siviller arasındaki ayrım ilkesi; savaşan tarafları her zaman yasal olarak saldırıya uğrayabilecek kişiler şeklindeki savaşçılar ile düşmanlıkların etkilerinden korunması ve esirgenmesi gereken kişiler şeklindeki siviller arasında ayrım yapmaya mecbur eden bir ilkedir. Bu ilke uyarınca silahlı bir çatışma söz konusu olduğunda her bir birey ya meşru bir askeri hedef olarak yahut da silahlı çatışmadan korunması gereken kişi olarak nitelendirilecektir. Bu ilke; silahlı çatışmanın tüm topluma nüfuz etmeyeceği, silahlı çatışmadaki meşru amacın düşman tarafın askeri gücünü zayıflatmak ve düşman tarafı yenmek olduğu fikrinin tezahürüdür⁴⁰.

Siviller ile muharipler arasındaki ayrım ilkesi, sivillerin korunması amacıyla getirilmiş bir ilke olmakla birlikte bu ilke sivillerin zarar görmemesini sağlama işlevini değil sadece “hedef alınmaması” işlevini görebi- lecek niteliktedir. Zira meşru bir saldırının beklenmeyen bir sonucu olarak sivillerin zarar görmesi durumunda siviller ile muharipler arasındaki ayrım ilkesi ihlal edilmiş olmayacaktır⁴¹. Bu ilke “sivillerin hedef alınmaması” ile sınırlandırılmıştır. Bu bağlamda sivil ve askeri uydularla ilgili olarak hangi uyduların meşru askeri hedef için kullanıldıklarının tespit edilmesi, hangi uyduların hem sivil hem askeri amaçlı kullanıldıklarının belirlenmesi güçtür. Özellikle hem sivil hem askeri işlev yürüten uygulamaların artması ve bu tür uyduların sivil işlevlerinin önemi dikkate alındığında bir uydu sivil kullanımın yanında askeri kullanımı da haiz ise bu uydunun ayrım ilkesi kapsamında hedef alınması ilke ihlali olarak değerlendirilmeyebilecektir. Bununla birlikte ayrım ilkesine uygun olarak hedef

40 Nils **Melzer**, “The Principle of Distinction Between Civilians and Combatants”, The Oxford Handbook of International Law in Armed Conflict içinde, Düz. Andrew Clapham ve Paola Gaeta, Oxford Academic, 2014, s. 296.

41 Gabriel **Swiney**, “Saving Lives: The Principle of Distinction and the Realities of Modern War”, International Lawyer, S. 39, 2005, s. 734.

alınıp imha edilen çift kullanımlı bir uyduyu yok ederken veya etkisiz hale getirirken uydunun sivil amaçlı kullanımının da işlevsiz hale gelmesi nedeniyle ortaya çıkacak yan etkileri siviller üzerinde zarara neden olabilecektir. Bu bağlamda ayırım ilkesi, çift kullanımlı bir uyduyu hedef belirlemek için tek başına yeterli olmayabilir. Bu tür durumlarda ayırım ilkesine ek olarak “saldırıda orantılılık” ilkesinin de dikkate alınması gerekmektedir⁴².

Uyduya gerçekleştirilmesi planlanan siber saldırıya ilişkin olarak uydunun askeri kullanımda bir uydu olduğunun tespiti saldırının gerçekleşmesi için tek başına yeterli değildir. Askeri hedefe karşı gerçekleştirilecek bir saldırının orantılı olup olmadığının da değerlendirilmesi gerekmektedir. Özellikle hem sivil hem askeri işlevi olan uydular düşünüldüğünde söz konusu uydunun askeri kullanımının amaçlandığına dair yeterli istihbarat ve bilgi olması, uydunun askeri hedef olarak belirlenip saldırı gerçekleştirilmesi için yeterli görülmemelidir. Bu şekilde sivil işlevi de olan çift işlevli bir uydunun salt askeri işlevi de bulunması dolayısıyla hedef alınmasının Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişkin Protokol’ün 52. maddesi 2. fıkrası bağlamında hukuka uygun olduğunun savunulması, sivil halkı korumak yerine askeri etkinliği haksız yere önceliklendirmek anlamına gelecektir⁴³.

IV. SİBER SALDIRILARIN DIŞ UZAY ANLAŞMASI BAĞLAMINDA DEĞERLENDİRİLMESİ

Dış Uzay Anlaşması’nın (Anlaşma) VI. maddesi uyarınca anlaşmaya taraf devletlerin, ay ve diğer gök cisimleri de dahil olmak üzere uzaydaki ulusal faaliyetler için uluslararası sorumluluk taşıdıkları kabul edilmiştir. Madde uyarınca Anlaşma’ya taraf devletlerin sorumluluğu; uzaydaki faaliyetleri yürüten bağlamında devletle sınırlı olmayıp devlet dışı kuruluşlar tarafından yürütülen faaliyetleri de kapsamaktadır. Bir başka ifadeyle Anlaşma’ya taraf devletler, ulusal faaliyetlerin bu Anlaşmada belirtilen hükümlere uygun olarak yürütülmesini sağlamakla yükümlü olup ayrıca uzaydaki devlet dışı kuruluşların yürüttükleri faaliyetler için uluslararası

42 **Stephens /Steer**, s. 31; Hem sivil hem askeri amaçlı uyduların siber saldırıların hedefi olması halinde sivillerin görebilecekleri zararlar; sivil havacılıkta kullanılan GPS sinyallerinin bozulması, yüksek ölçüde uydu sinyallerine bağlı telekomünikasyon ve finansal işlemlerin, otomatik su şebekesi ve baraj sistemlerinin zarar görmesi gibi örneklendirilebilir. **Stephens /Steer**, s. 19

43 **Henry Shue, David Wippman**, “Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions”, *Cornell International Law Journal*, S. 35, 2002, s. 560.

sorumluluk taşımaktadır. Bu bağlamda uzayda devlet dışı kuruluşların faaliyette bulunabilmesi Anlaşma'nın aynı maddesi uyarınca taraf Devletin yetkilendirmesine ve sürekli denetimine bağlanmıştır⁴⁴. Diğer taraftan Anlaşma'da taraf devletin yetkilendirmesi ile sürekli denetimi gibi kavramların tanımı yapılmadığından ve Anlaşma'daki hükümlerin çok genel olmasından dolayı Anlaşma'nın dış uzay faaliyetlerinde Devletler tarafından önemsenmediği ve güncellenmesi gerektiği savunulmaktadır⁴⁵. Benzer şekilde Anlaşma'da aktörlerin net olarak tanımlanmaması nedeniyle Anlaşma'nın devletler ve devlet dışı aktörler üzerinde amaçlanan etkiyi doğurmayacağı belirtilmektedir⁴⁶.

Dış Uzay Anlaşması madde VI bağlamında uzayda devlet dışı aktörlerin faaliyet göstermesi tamamıyla yasaklanmamış olmakla birlikte taraf devletlerin yetkilendirmesi ve gözetiminde olması şartına bağlanarak serbest bırakılmıştır. Bir başka ifadeyle Anlaşma tarafı devletin yetkilendirmediği özel kuruluşların dış uzayda faaliyet göstermeleri yasaklanmıştır⁴⁷. Aynı madde metninde “international responsibility” olarak ifade edilen taraf devletin uluslararası sorumluluğuna işaret edilmiştir. Bu nedenle taraf devlet, uzayda faaliyet göstermesi için yetkilendirdiği devlet dışı aktörün uzayda gerçekleştirdiği faaliyetin hukuka uygun olacağına güven duymalı, faaliyetlerin bu Anlaşmada belirtilen hükümlere uymamasından kendisinin sorumlu olduğundan hareketle Anlaşma'ya aykırı faaliyetlerde bulunmayacağını değerlendirdiği aktörleri yetkilendirmelidir. Her bir devlet yetkilendirdiği ve denetlediği devlet dışı aktörün gerçekleştireceği uzay faaliyetinden sorumludur⁴⁸. Bununla birlikte farklı devletler tarafından yetkilendirilmiş farklı devlet dışı aktörlerin iş birliği yaparak bir faaliyet gerçekleştirmesi durumunda devlet dışı aktörleri yetkilendirmiş bulunan

44 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Washington, London, Moscow, 10 Ekim 1967.

45 Didem **Rodoplu Şahin**/Matluyba **Bebitova**, “Uzay Madenciliğine İlişkin Zorluklar ve Potansiyel Çözümleri”, Nişantaşı Üniversitesi Sosyal Bilimler Dergisi, C.10, S. 1, 2022, s. 175.

46 Ram S. **Jakhu**, “Application and Implementation of the 1967 Outer Space Treaty”, XXXX Colloquium on the Law of Outer Space, 1997, s. 444.

47 Tuğrul **Çakır**, “Türk Uzay Operasyonlarına İlişkin Kanun'un Hazırlanması Konusunda Öneriler”, Yıldırım Beyazıt Hukuk Dergisi, C. 5, S. 2, 2020, s. 178.

48 Anlaşma'nın VI. maddesinden hareketle devlet dışı aktörlerin, devletlerinin yapmasının yasak olduğu şeyleri yapmalarının yasak olduğu da evleviyetle kabul edilmelidir. **Jakhu**, s. 444

her bir devletin birlikte sorumluluğu gündeme gelebilecektir⁴⁹. Her ne kadar madde metninde yer alan “*the appropriate State*” şeklinde tekil ifade kullanımının lafzi yorumundan sorumluluk bağlamında Anlaşma’ya göre taraf devletlerden sadece birinin sorumlu olabileceği gibi bir durum anlaşılrsa da amaçsal yorumla hareket edilmeli somut olay dikkate alınarak birden fazla taraf devletin sorumluluğuna gidilebilmelidir. Doktrinde de maddede geçen uygun devlet (appropriate state) ile fırlatan devlet (launching state)in aynı devlet olması gerekmediği gibi VI. madde bağlamında tek bir devlet dışı aktörde birden çok taraf devletin sorumluluğuna gidilebileceği belirtilmektedir⁵⁰.

Uzay antlaşmaları kapsamındaki Devlet sorumluluğu ve uluslararası yükümlülük normlarının net ve gerçek etkilerinin belirlenebilmesi ise hükümlerin ifadesindeki muğlaklık ve bu bağlamda ortaya çıkan çeşitli yorumlar nedeniyle belirsizliğini korumaktadır⁵¹. Bununla birlikte genel olarak Dış Uzay Anlaşması’nın VI. maddesinin devlet dışı kuruluşların ulusal uzay faaliyetleri için Devletlerin doğrudan sorumluluğunu, sanki bu faaliyetler devletlerin kendi eylemleriymiş gibi belirlediği kabul edilmektedir. Burada belirtilmelidir ki uzay faaliyetleri dış uzay hava sahasında yapılan faaliyetlerle sınırlı değildir. Anlaşma’da yer alan ‘uzaydaki ulusal faaliyetler’ ifadesi yalnızca uzayda meydana gelen faaliyetlere ilişkin bir kapsam ifade etmemektedir. Örneğin Anlaşma’ya taraf devletlerin, Dünya’da gerçekleşen fırlatma faaliyetleri ‘uzaydaki’ faaliyetler olarak değerlendirilmektedir⁵². Bu nitelendirme uzay sistemlerinin kritik sivil aktivitelerde de kullanıldığı dikkate alındığında aslında uluslararası insani hukuk kapsamında izin verilmeyen imha saldırılarının dünya üzerinde gerçekleştirilmemekle birlikte uzay üzerinden gerçekleştirilerek daha kapsamlı bir zarar ve etki oluşturma tehlikesini doğrulamaktadır.

Uzaydaki faaliyetlerin tüm ülkelere etkisi nedeniyle barışçıl çerçevede gerçekleştirilmesi gerekmektedir. Uzayın barışçıl amaçlarla kullanılması

49 Feriha Beyza **Eryavuz**, “Uzay Hukukundaki Yükümlülük Rejimi Bağlamında Fırlatan Devlet Kavramı ve TURKSAT-5B Uydusu”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C. 9, S. 1, 2022, s. 36.

50 **Jakhu**, s. 444.

51 Sandeepa **Bhat B.**, “State Responsibility and International Liability”, International Space Law in the New Space Era: Principles and Challenges içinde, Dü. Dilip Ukey, Adithya Variath, Sandeepa Bhat B., Oxford Academic, Oxford, 2024, s. 105.

52 Motoko **Uchitomi**, “State Responsibility/Liability for ‘National’ Space Activities, Towards Safe and Fair Competition in Private Space Activities”, American Institute of Aeronautics and Astronautics Inc, 2001, s. 52.

konusunda uluslararası iş birliği önemli olup dış uzayda silahların konuşlandırılmasının yasaklanması ve uzayda bir silahlanma yarışının önlenmesi için 1978 yılında, Genel Kurul, onuncu özel oturumunun Sonuç Belgesi'nde, uzayda olası bir silahlanma yarışının içsel tehlikelerini kabul etmiş ve böyle bir olayın önlenmesi için daha fazla önlem alınması ve uygun uluslararası müzakerelerin yapılması çağrısında bulunmuştur⁵³. Doktrinde belirtildiği üzere Birleşmiş Milletlere göre uzayın askerî amaçlarla kullanımı 1967 Dış Uzay Antlaşması'nın ihlali anlamına gelmekte, BM'ye üye devletlerin uzaydaki faaliyetlerinde barışçıl amaçlar çerçevesinde hareket etmeleri ve muhtemel bir silahlanma durumunun potansiyel tehlikeleri ele alındığında uzayda silahlanma yarışı başlatmamaları gerekmektedir⁵⁴. Her ne kadar Dış Uzay Anlaşması ve diğer uluslararası iş birlikleri ile uzayın barışçıl çerçevede kullanımının sağlanması amaçlansa da bilişim teknolojilerindeki gelişmeler neticesinde dış uzayda devletler arası çeşitli tekniklerle barışçıl olmayan faaliyetler gerçekleştirilebilmektedir.

Ayrıca uzayın barışçıl kullanımı şeklinde ifade edilen “peaceful use of outer space” ifadesi Dış Uzay Anlaşması'nda tanımlanmamıştır ve devletlerin bu kavram üzerinde uzlaştığı bir durum söz konusu değildir. Zira “uzayın barışçıl kullanımı” ifadesi uzayın saldırgan olmayan kullanımı şeklinde düşünüldüğünde saldırgan olmayan savunma amaçlı askeri kullanımın mümkün olduğu şeklinde çıkarımda bulunulabilecektir. Öte yandan “uzayın barışçıl kullanımı” ifadesi uzayın askeri olmayan kullanımı şeklinde de yorumlanabilir. “Uzayın barışçıl kullanımı” üzerinde devletlerin üzerinde uzlaştığı bir kapsam ve tanım bulunmaması diğer Devletlerin bunu zaten yapmış olabileceği korkusu nedeniyle Devletleri daha geniş yoruma doğru hareket etmeye teşvik etme riski taşımaktadır. Bu şekilde uzaydaki izin verilen faaliyetlerin geniş yorumlanması ise elektronik savaş ve siber savaş teknolojilerinin geliştirilmesine ve kullanılmasına izin verilmesi anlamına gelmektedir⁵⁵.

V. SİBER SALDIRILAR SONUCU UZAYDA DOĞAN ZARARDAN SORUMLULUK

Uzayda yapay zekâ gibi modern gelişmeleri açıkça ele alan yeni bir uzay anlaşmasının yapılması gerektiği önerilmektedir. Uzayda kullanılan yapay zekâ sistemlerinin etik ilkelere uygun olması gerektiği yönündeki

53 United Nations. United Nations Juridical Yearbook, United Nations, 1981, s. 47.

54 Mehmet Erkan Kılıçoğlu, “Uzay Hukuku, Uzayda Güvenlik ve Diplomasi”, İletişim ve Diplomasi, S. 12, 2024, s. 101.

55 Rajagopalan, s. 12, 13.

yaklaşımında etik ilkelere uygunluğun özdenetim mekanizmaları üzerinden yapılması gerektiği yönündeki savın uygulamada etkili olmayacağı, bunun yerine dış denetim anlayışının benimsenmesi gerektiği savunulmaktadır. Zira yapay zekâ sistemlerinin kullanımının etik ilkelere uygun olup olmadığının iç denetim şeklinde yapay zekâ sistemini kullanan kurum veya devletlerin özdenetimi şeklinde yapılması yerine dış denetimin ve uzayda yapay zekâ kullanımına dair ayrı bir anlaşma şeklinde hukuki düzenlemelerin etkili olduğu bir mekanizma kurulması durumunda yapay zekanın insan haklarını ihlal etmesinin önlenebileceği düşünülmektedir. Bu bağlamda ortak kurallar oluşturularak dış denetim ve gözetimin sağlanmasında Birleşmiş Milletlerin yetkilendirilmesi gündeme gelebilir. Teknoloji şirketlerinin yapay zeka ürünleri üretirken bilişim teknolojilerinin temel insan haklarını ihlal etmemesini, endüstri 4.0da insan haklarına saygı gösterilmesi ve insan haklarının korunmasını sağlamak için uymaları gereken ortak kuralların belirlenmiş olduğu Birleşmiş Milletler İş ve İnsan Hakları Rehber İlkeleri gibi uzayda ortak faydanın sağlanması amacıyla uzay faaliyetlerinde insan haklarına saygı gösterilmesi ve insan haklarının korunmasını sağlamak için devletlerin uymaları gereken ortak kuralların belirlendiği düzenlemeler yapılması gerektiği savunulmaktadır⁵⁶.

Uzay faaliyetlerinde yapay zekâ sistemlerinin kullanımına ilişkin ortak bir düzenleme yapılması konusunda uzlaşılmış bir siyasi iradeye ihtiyaç olduğundan ve henüz bu yönde devletler arası bir uzlaşma iradesi mevcut olmadığından uzay faaliyetlerinin işlevsel olması ve siber saldırıların önlenmesi amacıyla Dış Uzay Anlaşması gibi mevcut anlaşma yükümlülüklerinin kılavuzlar ile açıklığa kavuşturulması ve iş birliği ile güven artırıcı önlemler ile desteklenmesi önerilmektedir⁵⁷.

Dış Uzay Anlaşması'nın 3. maddesi dolayısıyla uluslararası hukukun uzaydaki faaliyetlere aktarımı ve örf ve âdet hukukunun uluslararası hu-

56 Larysa **Soroka**/Kseniia **Kurkova**, "Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues", *Advanced Space Law Journal*, S. 3, 2019, s.137, 138.

57 Thomas **Graham**/Kathiravan **Thangavel**/Anne-Sophie **Martin**, "Navigating Alien Terrain: Legal Liability for Artificial Intelligence in Outer Space", *Acta Astronautica*, S. 217, Nisan 2024, s.198.

kuk düzeyine ulaşması halinde yeni normların tanınması mümkün olmakla birlikte⁵⁸, bu durum; uzay gibi nevi şahsına münhasır bir alana herhangi bir uluslararası hukuk ilkesinin uygulanmasına izin verecek şekilde kapsayıcı bir hüküm olarak yorumlanmamalıdır⁵⁹.

Dış Uzay Anlaşması'nın VII. maddesini genişletici etkideki Sorumluluk Sözleşmesi (The Liability Convention) uyarınca, fırlatan Devletler, meydana gelen herhangi bir hasardan müştereken ve müteselsilen sorumludur. Bu Sözleşme; Devletleri riskleri en aza indirerek en iyi uygulamalara teşvik edici ve uluslararası antlaşma yükümlülüklerine uymaya yönelik niteliktedir. Bu bağlamda risklerin minimize edilmesi ve uzay faaliyetlerinin iyileştirilmesi için bu Sözleşme, devletler üzerinde uygun ulusal uzay mevzuatı geliştirmeye motive edici etkiyi haizdir⁶⁰.

Yapay zekâ destekli bir uzay nesnesini fırlatan devlet, söz konusu nesne tarafından yahut söz konusu uzay nesnesinde bulunan bir yapay zekâ sistemi nedeniyle verilen zarardan “fırlatan devlet” uyarınca sorumlu olmalıdır. Bu nedenle yapay zekâ destekli uzay nesnelerini fırlatan devletlerin bunlardan kaynaklı doğabilecek zararı önlemeye yönelik özen yükümlülüğü bulunduğu kabul edilmelidir. Bu durumda yapay zekâ sistemlerini barındıran uzay nesneleri kendi topraklarından fırlatılan Devletlerin tüm 'akıllı' uzay nesnelerini yetkilendirme ve denetlemeleri gerekmektedir. Bu bağlamda devletlerin yapay zekâ barındıran uzay nesnelerine ilişkin özen yükümlülüğünün kapsamı geniş olarak değerlendirilmelidir. Devletlerin yapay zekâ destekli uzay nesnelerinin siber saldırılara, kesintilere veya otomatik navigasyon ve iletişim sistemlerini etkileyecek şekilde başka şekilde tehlikeye atılmasına karşı güvenliğini sağlamaktan sorumlu olmaları bu kapsamda değerlendirilmelidir⁶¹.

Devletlerin özen yükümlülüğü kapsamında zarardan sorumluluğu yalnızca kendi yapay zekalı uzay nesnesinde bulunan yapay zekâ sistemlerinin korunmasına yönelik olmamalıdır. Yapay zekâ destekli sistemler tarafından uzayda başka devletlerin nesnelerine yahut başka devletlerin yer-yüzündeki teknolojilerine siber saldırıların gerçekleştirilmesi yahut başka devletlerin sistemlerini kesintiye uğratici, bozucu, yanıltıcı uygulamaların olması halinde bu tür faaliyetleri gerçekleştiren akıllı uzay nesnesini fırlatan devletin sorumluluğuna gidilmelidir.

58 Bu durum devletlerin bir uygulamasının örf ve âdet hukuku kuralı haline gelmesi şeklinde doktrinde “*opinio juris*” olarak ifade edilmektedir.

59 **Graham/Thangavel/Martin**, s.199.

60 **Graham/Thangavel/Martin**, s.199.

61 **Graham/Thangavel/Martin**, s.199.

Siber saldırıların, doğası gereği, bir saldırı gerçekleştikten sonra bile tespit edilmesi veya izlenmesi kolay değildir. Bu tür saldırı iddialarının tarafsız bir şekilde tahkim ile çözülmesi bir öneri olarak düşünülebilir. Bu durum; 30.11.2012 tarihli “Ulusal ve Uluslararası Düzeyde Hukuk Devleti Üzerine BM Genel Kurulu’nun Üst Düzey Görüşme Bildirisi ile kabul edilen devletlerin uluslararası anlaşmazlıklarını arabuluculuk, uzlaştırma, tahkim gibi barışçıl yollarla çözmesi anlamına gelen *uyuşmazlıkların barışçıl yollarla çözülmesi* ilkesiyle de örtüşecektir⁶². Bazı durumlarda bu tür tarafsız tahkim mekanizmaları kullanılmakta ise de, bu şekilde tahkime gidilmesi dış uzayda gerçekleştirilen siber saldırılarda bir temel norm olarak benimsenmemiş olup daha ziyade istisnai bir yol olarak kabul edilmiştir. Dış uzayda gerçekleştirilen siber saldırılarda sorumluluğun belirlenerek zararın giderilmesi için, uluslararası meşruiyete sahip olacak küresel katılımı teşvik etmek üzere BM yetkisine sahip bir kurumun tahkim merkezi olarak işlev görmesinin etkili olacağı düşünülmektedir⁶³.

SONUÇ

Bilişim teknolojilerinin uydular üzerine yerleştirilerek yahut yeryüzü destekli olarak uydular üzerinde siber saldırıların gerçekleştirilmesinde etkin olarak kullanıldığı durumlarla karşılaşılmaktadır. Siber saldırılar doğrudan uydulara sızılarak uydudaki sistemlerin etkisiz hale getirilmesi şeklinde olabileceği gibi kullanıcıların hedef sinyali almasının engellenmesi, veri akışına yanlış bilgi enjekte edilmesi, uydulara yanlış komutlar verilmesi gibi farklı şekillerde gerçekleştirilebilmektedir. Siber saldırılar uydunun tamamen ve süresiz olarak işlevsiz hale gelmesini sağlamaktan ziyade genellikle kısa süreli işlevsiz hale gelmesini sağlamak yahut kısa süreli yetkisiz erişim sağlanarak uydulara farklı komutlar vermek veya veri toplamak gibi belirli süreli olarak gerçekleştirilmektedir. Bu nedenle bir uydunun üzerinde gerçekleşen müdahalenin kasıt içermeyen kazara bir müdahale mi olduğu yoksa kasten gerçekleştirilmiş bir siber saldırı mı olduğunun ayırt edilebilmesi çok zordur. Her ne kadar 1978 yılında, Birleşmiş Milletler Genel Kurulu, onuncu özel oturumunun Sonuç Belgesi’nde, uzayda olası bir silahlanma yarışının oldukça riskli olduğu belirtilmiş ve bunun önlenmesi için gerekli tedbirlerin alınması çağrısında bulunmuş olsa da ve Birleşmiş Milletlere göre uzayın askerî amaçlarla kullanımı

62 Sezercan **Bektaş**, “Hukukun Üstünlüğü İlkesinin Avrupa Birliği (Ulus-Üstü) Hukukuna Aktarımı ve İlkenin Normatif Muhteviyatının Tespiti Sorunu”, Hacettepe Hukuk Fakültesi Dergisi, C. 12, S. 1, 2022, s. 819, 820.

63 **Rajagopalan**, s. 18.

1967 Dış Uzay Antlaşması'nın ihlali anlamına gelmekte ise de bilişim teknolojilerinin uzay faaliyetlerinde kullanımının silah yarışı haline geldiği değerlendirilmektedir. Zira uydular üzerinde gerçekleştirilen birçok siber saldırı casusluk yapılması yahut altyapının bozulması gibi askeri amaçla gerçekleştirilmektedir. Bu bağlamda birçok uydu üzerinde yapay zeka destekli yazılım veya cisimlerin yerleştirildiği ve bunların da siber saldırılarda kullanılabilirdiği değerlendirilmektedir.

Uzayda gerçekleştirilen askeri siber saldırılarda astronotun durumuyla ilgili olarak astronotun kendisinin savaş eylemlerine katılmadığı durumlarda, uzay hukuku kapsamında insanlık elçisi olarak değerlendirilmeli ve askeri personel olsa dahi astronot askeri nitelikli siber saldırıyı kendisi gerçekleştirmediği durumda koruma altında olmalıdır.

Kinetik saldırılar için ciddi yatırımlar gerektiği halde ve devletler gibi büyük maliyete katlanabilecek tüzel kişiler için kinetik saldırıdan şüphelenebileceği halde siber saldırıların az maliyetli olması, bunların devlet dışı aktörler tarafından da gerçekleştirilmesine olanak tanımaktadır. Bu durumda devlet dışı aktör tarafından gerçekleştirilen bir siber saldırıda saldırıyı gerçekleştiren aktörün tespiti halinde Dış Uzay Antlaşması'nın VI. maddesi uyarınca her devlet yetkilendirdiği ve denetlediği devlet dışı aktörün gerçekleştireceği uzay faaliyetinden sorumlu olduğundan saldırıyı gerçekleştiren aktörün verdiği zarardan o aktörü yetkilendiren devlet sorumlu olmalıdır. Bununla birlikte siber saldırılar maliyeti az olmanın yanında anonimliğe elverişli olduğundan uzayda siber saldırıyı hangi aktörün gerçekleştirdiğinin tespiti son derece zordur. Siber saldırılar sonucu elde edilen veriler devletler için ciddi önem taşıyabildiğinden, doğrudan maddi bir zarar oluşmasa dahi güç dengelerini etkileyecek şekilde politik zararların doğması durumunda bu zarar ile uzayda gerçekleştirilen siber saldırı arasında illiyet bağının kurulması ve ispatı hemen hemen imkânsız olacaktır.

Siber saldırının bir yapay zekâ destekli akıllı uzay nesnesi tarafından gerçekleştirilmesi durumunda bunun yapay zekanın algoritması nedeniyle anlaşılamayan bir sonuç şeklinde mi olduğu, yapay zekâ destekli sistemi kullanan devlet veya devlet dışı aktör tarafından mı planlandığı, dışarıdan bir sızıntı sonucu mu gerçekleştirildiği ayırt edilmesi neredeyse imkânsız bir diğer sorundur. Bu tür tespit sorunları, sorumlunun ve sorumluluğun kapsamının belirlenmesini de zorlaştırmaktadır. Tespit gerçekleştirilebiliyor ise Sorumluluk Sözleşmesi (The Liability Convention) uyarınca, fırlatan Devletin sorumluluğuna gidilmelidir.

Tüm bu hususlar dikkate alındığında dış uzay faaliyetleri kapsamında siber saldırıların gerçekleşmesi durumunda gerekli araştırmanın yapılarak

doğru tespitlerin sağlanabilmesi ve BM Genel Kurulu'nun Üst Düzey Görüşme Bildirisi ile kabul edilen devletler arası uyuşmazlıkların barışçıl yollarla çözümlenmesi ilkesinin uygulamaya yansiyabilmesi için BM yetkisine sahip bir tahkim merkezinin yetkilendirilmesi önerilmektedir.

KAYNAKÇA

- Agre**, Philip E., “Imagining the Next War: Infrastructural Warfare and the Conditions of Democracy”, 15 Eylül 2001, <https://pages.gseis.ucla.edu/faculty/agre/war.html>, E.T. 01.01.2025.
- Arkin**, William M., “The Environmental Threat of Military Operations”, *International Law Studies*, S. 69, 1996, s. 116-135.
- Bektaş**, Sezercan, “Hukukun Üstünlüğü İlkesinin Avrupa Birliği (Ulus-Üstü) Hukukuna Aktarımı ve İlkenin Normatif Muhteviyatının Tespiti Sorunu”, *Hacettepe Hukuk Fakültesi Dergisi*, C.12, S.1, 2022, s. 810-863.
- Bhat B.**, Sandeepa, “State Responsibility and International Liability”, *International Space Law in the New Space Era: Principles and Challenges içinde*, Düz. Dilip Ukey, and Adithya Variath Sandeepa Bhat B., Oxford Academic, Oxford, 2024, s. 105–121.
- Bingen**, Kari A./**Johnson**, Kaitlyn/**Young**, Makena/**Raymond**, John, *Space Threat Assessment*, Center for Strategic and International Studies (CSIS), Washington DC, 2023.
- Çakır**, Tuğrul, “Türk Uzay Operasyonlarına İlişkin Kanun’un Hazırlanması Konusunda Öneriler”, *Yıldırım Beyazıt Hukuk Dergisi*, C. 5, S. 2, 2020, s.175- 196.
- Eryavuz**, Feriha Beyza, “Uzay Hukukundaki Yükümlülük Rejimi Bağlamında Fırlatan Devlet Kavramı ve TURKSAT-5B Uydusu”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 9, S. 1, 2022, s. 30-50.
- Graham**, Stephen, “Switching Cities off Urban Infrastructure and US Air Power”, *City*, C. 9, S. 2, 2005, s. 169-194.
- Graham**, Thomas/**Thangavel**, Kathiravan/**Martin**, Anne-Sophie, “Navigating AI-lien Terrain: Legal Liability for Artificial Intelligence in Outer Space”, *Acta Astronautica*, S. 217, Nisan 2024, s. 197-207.
- Güldoğan**, Mustafa Veysel/**İşikli**, Şevki, “Siber Savaşta Mütakabiliyet”, *AJIT-e: Academic Journal of Information Technology*, S. 51, (Kasım 2022), s. 287 - 319, E.T. 03.07.2024.
- Hanan**, J. Trenton/**Fowler**, Ethan/**Hernandez**, Sebastian/**Niemczyk**, Matthew/**Tatar**, Unal/**Keskin**, Omer Faruk, “Analysis of Satellite Systems’ Dependencies and Their Cascading Impacts”, *Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, ABD, s. 493-498.
- Hanke**, Heinz Marcus, “The 1923 Hague Rules of Air Warfare — A Contribution to the Development of International Law Protecting Civilians from Air Attack”, *International Review of the Red Cross*, Cambridge University Press, C. 33, S. 292, 2010, s. 12-44.
- Hays**, Peter L., “What Should the Space Force Do? Insights from Spacepower Analogies”, *Doctrine, and Culture, War and Peace in Outer*

Space: Law, Policy, and Ethics içinde, Düz. Matthew Hersch, Cassandra Steer, Oxford University Press, New York, 2021, s. 153-180.

İnan Şimşek, Aybüke/**Atvur**, Senem, “21. Yüzyılda Uluslararası Uzay Rejiminin İnsanlığın Ortak Mirası Temelinde Yeniden İnşası”, *Alternatif Politika*, C. 13, S. 3, 2021, s. 593-628.

Jakhu, Ram S., “Application and Implementation of the 1967 Outer Space Treaty”, XXXX Colloquium on the Law of Outer Space. 1997, s. 442-448.

Killoğlu, Mehmet Erkan, “Uzay Hukuku, Uzayda Güvenlik ve Diplomasi”, *İletişim ve Diplomasi*, S. 12, 2024, s. 91-109.

Martinez, Larry F., “The Legal and Policy Dimensions of Cyber-Conflict in Outer Space”, Düz. Y. Bayraktar, S. Alis, *Proceedings for the Second Symposium on Space Economy, Space Law and Space Sciences*, İstanbul, İstanbul University Press, 2023. s. 111-124.

Melzer, Nils, “The Principle of Distinction Between Civilians and Combatants”, *The Oxford Handbook of International Law in Armed Conflict içinde*, Düz. Andrew Clapham ve Paola Gaeta, Oxford Academic, 2014, s. 296-331.

National Air and Space Intelligence Center (U.S.), “Competing in Space, Federal U.S. Documents Collection, 2018.

O’Meara, Chris, “Anti-Satellite Weapons and Self-Defence: Law and Limitations”, Düz. L. Lindström, D. Giovannelli, K. Podiňš, D. Štruel C. Kwan. 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon), NATO CCDCOE Publications, Tallinn, Estonia, 2024, s. 249-262.

Pavur, James/**Martinovic**, Ivan, “The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space”, Düz. T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky, 2019 11th International Conference on Cyber Conflict: Silent Battle, NATO CCD COE Publications, Tallinn, Estonia, 2019, s. 1-18.

Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), *International Humanitarian Law Databases*. International Committee of the Red Cross, 8 Haziran 1977.

Rajagopalan, Rajeswari Pillai, *Electronic and Cyber Warfare in Outer Space*, The United Nations Institute for Disarmament Research (UNIDIR), Cenevre, 2019.

Robinson, Jana, “Prominent Security Risks Stemming from Space Hybrid Operations”, *War and Peace in Outer Space: Law, Policy, and Ethics içinde*, Düz. Cassandra Steer ve Matthew Hersch, Oxford University Press, New York, 2021, s. 229-246.

Rodoplu Şahin, Didem/**Bebitova**, Matluyba, “Uzay Madenciliğine İlişkin Zorluklar ve Potansiyel Çözümleri”, Nişantaşı Üniversitesi Sosyal Bilimler Dergisi, C. 10, S. 1, 2022, s. 171-188.

Shue, Henry/**Wippman**, David, “Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions”, Cornell International Law Journal, S.35, 2002, s. 559-579.

Soroka, Larysa/**Kurkova**, Kseniia, “Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues”, Advanced Space Law, S. 3, 2019, s. 131-139.

Steer, Cassandra/**Stephens** Dale, “International Humanitarian Law and Its Application in Outer Space”, War and Peace in Outer Space: Law, Policy, and Ethics içinde, Düz. Cassandra Steer ve Matthew Hersch, Oxford University Press, New York, 2021, s. 23-55.

Stephens, Dale/**Steer**, Cassandra, “Conflicts in Space: International Humanitarian Law and Its Application to Space Warfare”, McGill Annals of Air and Space Law, S. 40, 2015, s. 1-32.

Swiney, Gabriel, “Saving Lives: The Principle of Distinction and the Realities of Modern War”, International Lawyer, S.39, 2005, s. 733-758.

Swope, Clayton/**Bingen**, Kari A./**Young**, Makena/ **Chang**, Madeleine/**Songer**, Stephanie/ **Tammelleo**, Jeremy, Space Threat Assessment 2024, Center for Strategic and International Studies, Washington DC, 2024.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. Washington, London, Moscow, 10 Ekim 1967.

Uchitomi, Motoko, “State Responsibility/Liability for ‘National’ Space Activities, Towards Safe and Fair Competition in Private Space Activities”, PROC. COLLOQ. L. OUTER SPACE (American Institute of Aeronautics and Astronautics, Inc), 2001, s. 51-60.

United Nations, United Nations Juridical Yearbook, United Nations, 1981.

Zhou, Wen, “War, Law and Outer Space: Pathways to Reduce the Human Cost of Military Space Operations”, Humanitarian Law & Policy, 15 Ağustos 2023, s. 1-4.