

# Ön-Alıcı ve Önleyici Müdahalede Simülasyonlar

## Simulations in Pre-emptive and Preventive Intervention

Elif GÜRDAL LİMON\* - Onur LİMON\*\*

### Öz

*Simülasyonlar gerçek ortamların taklit edilmesi ve birebir benzerlerinin matematiksel modellerle yaratılması ile oluşturulan dijital ortamlardır. Bu dijital ortamlara gerçek dünyanın verileri yüklenerek yaşanabilecek tüm olasılıkların hesaplanabilmesi mümkün olabilmektedir. Ortaya çıkan bilginin ise gerçek dünyadaki politikaları etkileyebilmesi tartışılması gereken bir konu olmaktadır. Simülasyonlar sayesinde devletlerin önemli güvenlik meselelerine dair olasılık hesaplarının yapılması artık sık sık başvurulan yöntemler haline gelmiştir. Ancak dijital alan üzerinden sağlanmaya çalışılan bu güvenlik yönteminin savunma dayanağı olarak yönlendirici olup olmayacağı ya da simülasyon verilerine dayanarak bir eylemde bulunmanın saldırı olarak yorumlanıp yorumlanamayacağı tartışılmalıdır. Bu çalışma bu sorulara yanıt aramak için ele alınmıştır. Kavramsal çerçevede ön-alıcı ve önleyici müdahale kavramlarıdır. Bu çerçevede simülasyon verilerinin müdahale ederken bir savunma dayanağı olarak kullanılmasının ön-alıcı mı yoksa önleyici mi olduğu tartışılmaktadır. Simülasyon verileri ve yapay zekâ analizlerinin düşman tanımlaması ve saldırganlık göstergelerinin hesaplamalarında meşru bir hukuksal dayanak olup olamaması uluslararası iş birliğinin şekli ve uluslararası aktörlerin kabul edilir seçenekleri meşrulaştırma süreçlerine göre değişmektedir.*

**Anahtar Kelimeler:** Ön-Alıcı Müdahale, Önleyici Müdahale, Simülasyon, Dijitalleşme, Güvenlik.

\* Dr. Öğr. Üyesi, Gümüşhane Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Uluslararası İlişkiler Ana Bilim Dalı, Gümüşhane, Türkiye, ORCID: 0000-0001-5110-6524, e-posta: [elif.gurdal@gumushane.edu.tr](mailto:elif.gurdal@gumushane.edu.tr).

\*\* Dr., Uluslararası İlişkiler Alanında Bağımsız Araştırmacı, Gümüşhane, Türkiye, ORCID: 0000-0002-4097-303X, e-posta: [onurlimon2538@gmail.com](mailto:onurlimon2538@gmail.com).

Geliş Tarihi / Submitted: 16.05.2023

Kabul Tarihi / Accepted: 25.07.2023



## **Abstract**

*Simulations are digital environments created by imitating real environments and creating similar ones with mathematical models. In this respect, it is possible to calculate all the possibilities that can be experienced by uploading the data of the real world to these imitated digital environments. The fact that the resulting knowledge can affect real-world policies is a subject that needs to be discussed. Thanks to simulations, probability calculations for important security issues of states have now become frequently used methods. However, it should be discussed whether this security method tried to be provided through the digital space will be a directing factor as a basis for defence or whether taking an action based on simulation data can be interpreted as an attack. This study undertakes to seek answers to these questions. The conceptual framework of the study is the concepts of pre-emptive and preventive intervention. In this context, the study examines whether the use of simulation data as a basis for defence in interventions can be a pre-emptive and preventive approach. The legitimacy of using simulation data and artificial intelligence analyses for identifying enemies and calculating aggression indicators depends on the specific forms of international cooperation and the processes through which international actors establish acceptable options.*

**Keywords:** *Pre-emptive Intervention, Preventive Intervention, Simulation, Digitization, Security.*

## **Giriş**

Uluslararası ilişkilerin teknolojik dönüşümünü; fayda, etki veya risk gibi farklı açılardan yorumlamak gerekmektedir. Yeni ekonomik sektörlerin oluşması ve iletişimde hızlı bir akışkanlığın sağlanması gibi faydalar varken internet erişiminin sınırlandırıldığı/kesildiği bir ortamda borsa ve yatırımlarla ilgili sorunların çıkması olasıdır. Askerî alandaki dijital dönüşümde ise güvenlik anlamında riskler oluşsa da benzer şekilde bu risklerle sınırlı bir değişim yoktur. Askerî alandaki risklerin yanında faydalara bakıldığında; askerî silah çeşitlenmesi, istihbarat edinimi, dijital eğitimler, iletişimde veri akışının hızlı olması gibi birçok konuda avantajlar da ortaya çıkmaktadır. Bunlar bir güç olarak yorumlanabilir.

Devletlerin güç tanımlarına artık dijital yetenekleri de dâhil etmek gerekmektedir. Savaş alanları kara, hava, deniz ve uzay olarak tanımlanırken buna dijital bir savaş alanı olan siber alan da eklenmiştir. Bu anlayışta güç türlerine de dijital yetenekler eklenmektedir. Çünkü dijital gelişmelerden faydalanmak uluslararası anlamda bir rekabet konusu olmaya başlamıştır.

Dijital güvenlik bu açıdan hem bir güç kaynağı hem bir rekabet konusu hem de bir ulusal güvenlik meselesi olmaktadır.

Yapay zekâ, makine öğrenmesi, simülasyonlar, artırılmış gerçeklik gibi konular devletlerin askerî, ekonomik, siyasi ve toplumsal alanlarda faydalanmaya çalıştıkları ve gelecek dış tehditlere karşı korunmaya çalıştıkları konulardır. Ayrıca diğer aktörlerle de rekabet ettikleri konulardır. İnsan hafızası ile mukayese edilemeyecek oranda büyük verilerin yer aldığı yazılımlar devletlerin politik analizlerinde yer edinmeye başlamıştır. Özellikle devletlerin karar alıcı organlarının devlet çıkarları için alacakları kararlar yaşamsal değerde olabilmektedir. Bu tür kararların devletlerin uluslararası konumlarına zarar vermeden güç artırıcı sonuçlar doğurması beklenmektedir. Simülasyonlardan ve yapay zekâ destekli sistemlerden faydalanılması bu noktada giderek tercih edilen bir seçenek olmaktadır.

Simülasyonlar politik analiz ve karar alma sürecinde destekleyici veriler sunması bakımından değerli olmaya başlamıştır. Ayrıca insan beynini taklit etme özelliği ile simüle olaylarda eğitimler verebilmesi bakımından askerî personel veya karar alıcıların eğitilmesinde de kullanılmaktadır. Yetenekli personelin eğitilebilmesi ve riskli kararlarda zararın gerçek hayata yansımayacak şekilde simüle ortamlardan test edilmesi mümkün hale gelmiştir. Simülasyonlar bu açıdan gerçek hayatta riskli olabilecek operasyonların sonuçlarını önceden analiz edebilmek, gerçekçi eğitimler verebilmek, risk analizi yapabilmek için matematiksel hesaplamaların yapıldığı devletlerin en önemli başvuru kaynaklarından biri haline gelmektedir. Savaş konusunda ise bu simülasyon verilerinin gerçek hayata yansıtılması bir çelişkiyi doğurmaktadır. Bu durum uluslararası ilişkilerde savaş, güvenlik, savunma gibi önemli alanlardaki kavramların tanımlarıyla teknolojinin gelişmesiyle uluslararası ilişkiler eylemlerindeki tutarlılık sorunundan kaynaklanmaktadır.

Kimi durumda devletlerin korku tanımlaması ve düşman aktör tespiti algıya dayalı ve sezgisel olabilmektedir. Elbette ki uluslararası ilişkilerde savaş sebebi ve meşru müdafaa dayanakları tarihte olagelen uygulamalara bakıldığında belirli bir çerçeveye göre ilerlemektedir. Ulusal çıkarlara, toprak bütünlüğüne veya egemenlik haklarına yönelik ihlaller önemli ilk saldırı dayanağı olabilmektedir. Ancak net olmayan ve kanıtlarla sunulamayan durumlarda, bir devletin kendi ulusal çıkarlarına risk olarak gördüğü bir düşman tanımlaması ve kuvvet içeren ilk müdahalede bulunması tartışmalı olmakla beraber karşılaşılan uluslararası ilişkiler gelişmeleridir.

Matematiksel olarak bir devletin başka bir devlete saldırı yapma olasılığı hesaplanabilir mi? Bir devletin güç yükselişi tehdit olarak tanımlanıp bir başka devleti işgal edebilme olasılıkları ölçülebilir mi? En önemlisi de bu olasılık hesaplamaları gerçek hayatta bir dayanak olarak kullanılabilir mi? Çalışma bu tür sorulara yanıt aramak için hazırlanmıştır. Bunun için çalışma, meşru müdafaa kavramlarından olan ve 11 Eylül terör saldırıları ile akademik olarak tartışılması daha yoğun olan ön-alıcı müdahale ve önleyici müdahale<sup>1</sup> doktrinleri üzerinden ele alınmıştır.

Teknolojik gelişmelerin etkisini incelemek akademik anlamda uluslararası ilişkiler Türkçe literatürünün güncelliğini korumak ve dinamikliğini sağlamak içindir. Ayrıca askerî anlamda devletlerarasındaki çatışmacı süreçlerin tehdit analizini dijital teknoloji destekli bilimsel dayanaklarla ölçülebilir yapılması devletlerin ihtiyaç duyduğu yeni konulardır. Bu konuların karar alma süreçlerinde değerli olduğu ve daha da değerli olacağı düşünülmektedir. Simülasyonların bir devletin karar alma sürecinde dayanak olarak kullanılması ya da kullanılmaması üzerine yapılan bu çalışmanın hem bir ilk olması hem de ihtiyaç gidermesi bakımından Türkçe literatüre katkı yapacağı düşünülmektedir. Simülasyon alanını özellikle son dönemlerde savunma sanayi bakımından atak yapan Türkiye'nin jeopolitik konumu düşünüldüğünde askerî eğitim, karar alma süreçleri ve bölgesel risk tespiti bakımından kullanması değerli olacaktır.

Çalışma; kavramsal olarak ön-alıcı ve önleyici müdahale kavramlarının tanımlanması ile başlamaktadır. Ardından uluslararası ilişkilerde dijital güç yorumlaması yapılmış, bu alanda simülasyonların önemine, örneklerine ve işlevine yer verilmiştir. Daha sonra simülasyonların uluslararası ilişkilerde bir dayanak olarak kullanılabilirliği sonuç ve tartışma kısmında tartışılmıştır.

### **1. Ön-alıcı/Önleyici Müdahale Doktrini ve Dayanakları**

Uluslararası çatışmada ve anlaşmazlıkların çözümünde savaşa başvurmak tarih boyunca önemli bir yöntem olmuştur. Savaş, güç kapasitesine göre değişkenlik göstermekle birlikte başvurulmuş veya başvurulmaktan kaçınılan bir durumdur. Saldırı ve savunma arasında bu açıdan farklılıklar

---

<sup>1</sup> Kavramlar, bazı kaynaklarda ön-alıcı/önleyici savaş, ön-alıcı/önleyici vuruş, ön-alıcı/önleyici saldırı gibi farklı kelime grupları ile kullanılmaktadır. Bu çalışmada savaş ve saldırı kavramlarının yanlış anlaşılmaya mahal vermemesi için "ön-alıcı müdahale ve önleyici müdahale" ifadesi tercih edilmiştir.

vardır. Güç kapasitesinin görece üstünlüğü çoğu zaman saldırıda bir itici unsur olmuş, savunma ise zorunlu bir seçenek haline gelmiştir. Bu açıdan saldırının dayanakları önemli uluslararası ilişkiler alan inceleme konusu olmuştur. Uluslararası hukuk kurallarının yaratılması ve diplomasi ile sorunların savaşa başvurulmadan çözümlenmesi beklenmektedir. Ancak sorunların bu hukuk kurallarına göre giderilmesi ve çıkarların diplomasi masasında pazarlık edilerek çatışmaya varmadan çözümlenmesi bir seçenektir. Savaş olgusu halen daha uluslararası ilişkilerin politik sonuçlarından biridir.

Birleşmiş Milletler (BM) üye devletlere kuvvet kullanımından kaçınmayı kurallara göre belirlemiştir. BM Antlaşmasınının 51. maddesinde de belirtildiği gibi bu kuvvet kullanımından kaçınmanın istisnai durumu ise meşru müdafadır. Barışı ve istikrarı bozucu kuvvet kullanılan devlet(ler)e karşı kuvvet kullanımının yolu açılmaktadır. BM antlaşmasına göre kuvvet kullanımının “eyleme geçmiş” olması gerekmektedir. Eyleme geçmiş bu kuvvete karşılığı, bir devletin tek olarak veya diğer devletlerle birlikte kuvvet kullanımı ile verebilmesi mümkündür.<sup>2</sup> Kuvvet kullanımının meşru müdafaa hakkı ile meşrulaştırılması halen tartışmalı olmaktadır. Meşru müdafaa dayanağı olarak kuvvet kullanımı konusu olan ön-alıcı (*preemptive*) ve önleyici (*preventive*) müdahale kavramlarının tartışmaları bu açıdan karmaşıklaşmaktadır.

Ön-alıcı müdahale bir düşmanın saldırı yapmak için giriştiği bazı hazırlıkların fark edilmesiyle o düşmana karşı kuvvet içeren bir müdahalede bulunulmasıdır.<sup>3</sup> Bu müdahalenin yapılmasında düşmanın saldırı için bazı hazırlıklarının tespit edilmiş olması kanıt niteliğindedir. Ancak önleyici müdahale temel olarak bir düşman unsurunun saldırı hazırlığının kanıtlanmadığı, saldırı hazırlığının olup olmadığı belirlenemediği durumda dahi varsayım dayalı yapılan kuvvet içeren bir müdahaledir.<sup>4</sup>

Tarihte ön-alıcı müdahale örnekleri kanıtlanabilirlik bakımından halen günümüzle benzer niteliktedir. II. Dünya Savaşı esnasında, Temmuz 1940'ta, Birleşik Krallık Başbakanı Winston Churchill'in Cezayir'in Oran

<sup>2</sup> Hüseyin Pazarıcı, *Uluslararası Hukuk*, Turhan Kitabevi, Ankara, 2015, s. 120.

<sup>3</sup> Karl P. Mueller et al., *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*, RAND Corporation, Santa Monica, 2006, s. 5.

<sup>4</sup> James B. Steinberg, Michael E. O'Hanlon, Susan E. Rice, “The New National Security Strategy and Preemption”, 2002, <http://www.brookings.edu/comm/policybriefs/pb113.htm>, erişim 29.06.2023.

şehrinde bulunan Vichy Fransız filosuna yaptığı saldırı örnek gösterilebilir.<sup>5</sup> O dönem Fransız Cezayiri, Hitler Almanyası tarafından işgal edilmiştir. Churchill, Fransız Bakanın Fransız donanmasını Hitler'e teslim edeceği tehlikesine karşı ön-alıcı bir müdahale yaparak ilk saldırıyı yapmıştır. Bakan böyle bir iddiayı reddetse de Churchill'in haklı olduğu düşünülmüş ve filonun Hitler'e geçmeden ön-alıcı bir müdahalenin doğruluğu savunulmuştur.<sup>6</sup> Kaldı ki bu durumun ön-alıcı müdahale olarak görülmesinde önemli bir unsur II. Dünya Savaşı'nın hâlihazırda olması ve Hitler'in yayılmacı politikasının kanıtlanmış olmasıdır.

Diğer yandan tarihte önleyici müdahaleyi meşrulaştırmak için saldırılarda bulunan devletlerin hukuk dışı davranışları da söz konusu olmuştur. Buna da İsrail'in Haziran 1981 tarihinde Irak'taki Osirak reaktörünü bombalaması gösterilebilir. Bu olay 1981 yılında İsrail'in Irak'a yönelik Opera Operasyonu'nda gerçekleşmiştir. İsrail, Irak'ın o dönem Fransa'dan satın aldığı nükleer reaktörü nükleer silah geliştireceği düşüncesiyle tehdit olarak yorumlamıştır. Bu yüzden Opera Operasyonu ile Irak'a hava saldırısı yapmıştır.<sup>7</sup> İsrail bu saldırıyı önleyici meşru müdafaa olarak duyurup savunmuştur.<sup>8</sup> Irak'ın İsrail'e bir tehdit olarak görüldüğü iddia edilmiştir. Fakat Irak'taki bu reaktör o tarihte henüz kullanıma dahi alınmamış, hatta açılmamıştır.<sup>9</sup> Bu açıdan Irak'ın eylemleri ön-alıcı müdahale için bir kanıt niteliğinde olamadığından İsrail yine de önleyici meşru müdafaa iddiası ile bir meşrulaştırma sağlamaya çalışmıştır. Dolayısıyla bu eylem BM Güvenlik Konseyi tarafından oy birliği ile kınanmıştır.<sup>10</sup>

Devletlerin kuvvet kullanımı ve buna meşru müdafaa hakkı ile karşılık verilmesi basit bir açıdan yukarıda bahsi geçildiği gibi izah edilse de günümüzde bu durum daha karmaşık bir hal almıştır. Bu sürecin dönüm

---

<sup>5</sup>Thomas Parker, "When Churchill Bombed France." *The National Interest*, no. 145, 2016, s. 77-84.

<sup>6</sup> Kaufman ve Robert Gordon, *In Defense of the Bush Doctrine*, The University Press of Kentucky, Kentucky, 2007, s. 91-92.

<sup>7</sup> Joshua Kirschenbaum, "Operation Opera: An Ambiguous Success." *Journal of Strategic Security*, 3: 4, 2010, s. 49-62.

<sup>8</sup> Dan Reiter, "Preventive Attacks Against Nuclear Programs and the 'Success' at Osirak", *Nonproliferation Review*, 12:2, Haziran 2005, s. 355-371.

<sup>9</sup> Donald G. Boudreau, "The Bombing Of The Osirak Reactor" *International Journal on World Peace*, 10: 2, 1993, s. 21-37.

<sup>10</sup> United Nations Security Council Official Records, Attack on Iraq – SecCo Debate – Verbatim record, 2282nd Meeting: 15 June 1981, New York; United Nations Security Council, Decision of 19 June 1981 (2288th meeting): Resolution 487 (1981)

noktası ise 2001 yılındaki 11 Eylül terör saldırıları olmuştur. Soğuk Savaş'ın bitimi ile 1990'larda ABD'nin tek süper güç algısını karşılıklı rıza vurgusunun öne çıktığı iyicil hegemonya üzerinden yürütmeye çalışmıştır. İyicil hegemonya ABD'nin Soğuk Savaş sonrası insan hakları, demokrasi ve serbest piyasa ekonomisi gibi temeller üzerinden diğer aktörlere rıza sağlayarak asayiş görevini üstlenmesidir. Bu hegemonya rolünde diğer aktörlere bir hareket kabiliyeti de tanınır. İyiyi gözeten bir hegemonya rolü sunulur.<sup>11</sup> Bu süreç, iş birliği ve buna diğer aktörlerin teşvik edilmesi ile sürdürülmeye çalışılmıştır.<sup>12</sup> Bunu o dönemin ABD Ulusal Güvenlik Strateji (UGS) belgelerinde görmek mümkündür. 1993-2001 yılları arası ABD Başkanı olan Bill Clinton dönemi Strateji belgelerinde diplomasinin kullanılması gerekliliği ve ABD'nin güvenlik tehditlerine tek başına karşılık vermesinden ziyade iş birliğine gitmesi gerekliliği vurgulanmıştır.<sup>13</sup> Bu politikaların üzerinden 10 yıl geçmeden ise daha farklı bir ABD dış politikası ortaya çıkmış, bunda da 11 Eylül 2001 terör saldırıları etkili olmuştur. 11 Eylül'de gerçekleşen terör saldırısından hemen sonra dönemin ABD Başkanı George Bush'un ismini alan Bush Doktrini ilan edilmiş ve ulusal televizyonlarda teröristler ile teröre destek veren devletlerin kastedildiği terör destekçileri arasında ayırım yapılmayacağı duyurulmuştur.<sup>14</sup> 11 Eylül saldırılarından dolayı gerçekleşen bu gelişmeler ABD'nin küresel üstünlüğünü korumak için gideceği kuvvet kullanımına dayalı politika değişikliğinin dayanağı haline gelmiştir.<sup>15</sup>

11 Eylül ile birlikte, Soğuk Savaş'ın özü olan caydırıcılık ve çevreleme politikalarının yerine yeni stratejiler belirlenmeye başlanmıştır. Çünkü 2001-2009 yılları arasında ABD Başkanı olan George W. Bush döneminde Soğuk Savaş'ın çevrelenecek bir tehdit anlayışı yerini, nereden ve ne zaman geleceği belli olmayan bir tehdit algısına bırakmıştır.<sup>16</sup> Geleneksel çevreleme

<sup>11</sup> Lobel, Jules, "Benign Hegemony? Kosovo and Article 2(4) of the U. N. Charter," *Chicago Journal of International Law*, 1:1 Article 5, 2000, s. 25-27.

<sup>12</sup> Bülent Sarper Ağır, "Bush Doktrini Küresel Bir Hegemonik İstikrar Arayışı mı?," *Uluslararası İlişkiler*, 3:12, 2006, s. 71-100.

<sup>13</sup> The USA National Security Council, the National Security Strategy September 2002 Chapter III. Strengthen Alliances to Defeat Global Terrorism and Work to Prevent Attacks Against Us and Our Friends

<sup>14</sup> Walter Lafeber, "The Bush Doctrine", *Diplomatic History*, 26:4, 2002, s. 543-558.

<sup>15</sup> Patricia L. Dunmire, "9/11 Changed Everything: on Intertextual Analysis of the Bush Doctrine", *Discourse & Society*, 20:2, 2009, s.195

<sup>16</sup> Suat Dönmez, "Kuvvet Kullanma Kapsamında Ön Alıcı ve Önleyici Saldırı

ve caydırıcılık modelinin haydut devletlerde ve teröristlerde işe yaramayacağına inanılmaktadır. Bu da kuvvet kullanımının önünü açmaktadır. Çünkü teröristlerin motivasyonu, davaları için ölmeye dayalı manevi bir güçtür.<sup>17</sup> Böylelikle karmaşık ve tehdidin merkezini belirlenmesinde zorlukların yaşandığı terör konusunun devletlerin önemli güvenlik meselesi haline geldiği iyice belirginleşmiştir.

Tek kutuplu yapıda rakip hegemon güçlerin doğması daha olasıdır. Bu açıdan ABD hegemonyasına rakiplerin doğmasına daha olanaklı bir ortam olması ABD hâkimiyetindeki bir dünya sisteminin işlemede zorluklara neden olmuştur. İyicil hegemonya diğer devletlerin hegemon güce rakip olabilecek potansiyel rakiplere ortam açabilecektir.<sup>18</sup> Soğuk Savaş döneminde kullanılan caydırıcılık ve çevreleme politikaları Soğuk Savaş'ın sonrası iş birliği ve diplomasi ile tek kutuplu yapı üzerinden başka versiyonda devam ettirilse de Bush dönemi ile yeni muhafazakâr politikaların öne çıkması tüm bunlardan bir ayrılığı göstermiştir.<sup>19</sup> Bush Doktrini olarak addedilen önleyici müdahale (savaş) stratejisi ile çok taraflılık uluslararası örgütler ve uluslararası iş birliği yerine tek taraflı önleyici güç kullanımına geçilmiştir. Böylece 11 Eylül sonrası ABD Bush yönetiminin politikası önleyici ve ön-alıcı müdahale üzerine kurulmuştur.

Ön-alıcı müdahale ile önleyici müdahale arasından farklılıklar olmasına rağmen kavram karışıklığı nedeniyle birbiri yerine kullanıldığı durumlar olmuştur. Akademik anlamda literatürde ve bürokratik söylemlerde halen daha bu iki kavramın birbiri yerine kullanıldığı görülmektedir<sup>20</sup> Ön-alıcı müdahale saldırı hazırlığında olan bir düşmana karşı askerî hareket yaparak onun yapacağı saldırının önüne geçmektir. Yani bir devletin diğer devletin kendisine saldırmakla ve ona büyük zarar vermekle tehdit ettiği sonucuna vardıldıktan sonra diğerine askerî saldırı başlatmasıdır. Bu durum nefsi müdafaa olarak düşünülmekte ve haklı saldırı olarak görülmektedir. Uluslararası hukukta yer aldığı kabul edilmektedir. Diğer yandan önleyici müdahalenin

---

Kavramları”, *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi*, 3:3, 2017, s.10

<sup>17</sup> Ikenberry, G. John. “America’s Imperial Ambition.” *Foreign Affairs*, 81:5, 2002, s. 49.

<sup>18</sup> Layne, Christopher. “The Unipolar Illusion Revisited: The Coming End of the United States’ Unipolar Moment.” *International Security*, 31:2, 2006, s. 16

<sup>19</sup> Ağır, *Bush Doktrini*, s.73, s. 85

<sup>20</sup> Colin S. Gray, “The Implications of Preemptive And Preventive War Doctrines: A Reconsideration”, *USA Strategic Studies Institute U.S. Army War College*, Temmuz 2007, Başlık: 17, Bölüm: 101.



saldırganlık göstergesi olabileceği yorumu vardır. Uluslararası hukukta yer almadığı için hukuk ihlali olarak görülmektedir.<sup>21</sup> Karışıklık bu açıdan hukuk dışı olarak yorumlanan önleyici müdahalenin ön-alıcı müdahale olarak isimlendirilmesinden doğmaktadır. Yine de ayırım kesin, net ve basit değildir.

Ön-alıcı müdahale esasen tartışmalı olan kısım değildir. Ahlaki ve hukuki açıdan varlığı kabul görmüş bir yaklaşımdır. Hatta savaş kararının düşman tarafından zaten alınmış olduğu anlayışına dayanır.<sup>22</sup> Ön-alıcı müdahalede ilk saldırının yapılmasından başka seçenek kalmamakta, düşmanın kesin kanıtlara dayalı saldırısı bilinmektedir.<sup>23</sup> İlk vuruşun savunma maksadıyla gerçekleşmesi neredeyse kesin olan bir saldırıyı engellemek için yapıldığı müdahale türüdür. BM Antlaşmasına göre meşru müdafaa dayanağı olarak ele alınan ön-alıcı müdahale devletlerarası çatışmalarda belirgin tehdide yönelik bir ilk vuruş hamlesi olarak görülmektedir.<sup>24</sup> BM Antlaşması'nın 2. maddesi 4. fıkrası ile devletlerin birbirine karşı kuvvet kullanımı yasaklansa da meşru müdafaa hakkı ile BM 51. maddesi istisna tutulmuştur.<sup>25</sup>

Önleyici müdahale ise sezgisel ve güvenlik korkusu nedeniyle varsayılan düşman inancından kaynaklanmaktadır. Varlığı kesin kanıtlara dayanmamış olası düşman veya saldırı inancına dayandırılır. Endişeyle yaşamaktansa ilk vuruşu yaparak güvende hissetmek daha tercih edilebilir görülmektedir. Olası bir tehdidin ileride çıkabileceğine inanılmaktadır.<sup>26</sup> Ön-alıcı müdahalede yumruğu kaldırmış birinin o yumruğunu kesmek için yapılmasına karşın, önleyici müdahalede henüz karşıdaki yumruğu kaldırabilmek için kasları geliştirmekle meşgul olabilir. Önleyici müdahale yumruğu henüz kaldırmamış düşmana ileride tehdit olmasın diye yapılan müdahaledir.<sup>27</sup>

Önleyici müdahalede ön-alıcı müdahaledeki ilk vuruş hamlesinin saldırıyı engellemek için olan motive dayanağını farklı ele alındığı

---

<sup>21</sup> Matthew J. Flynn, *First Strike: Preemptive Warfare in Modern History*, Taylor & Francis, New York, 2008, s. 1-2.

<sup>22</sup> Karl P. Mueller vd., *Striking First*, s. xii.

<sup>23</sup> Gray, *The Implications of Preemptive And Preventive*.

<sup>24</sup> Ulaş Karadağ, "Birleşmiş Milletler Antlaşması'na Göre Meşru Müdafaa Hakkı", *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 7:2, 2016, s. 171-186.

<sup>25</sup> Charter of the United Nations, Chapter I, Purposes and Principles Article 2(1)-(5), <https://legal.un.org/repertory/art2.shtml>

<sup>26</sup> Gray Ibid.

<sup>27</sup> Alastair Finlan, "International Security", Mary Buckley ve Robert Singh, (ed.), *The Bush Doctrine And The War On Terrorism Global Responses, Global Consequences*, Routledge, New York, 2006, s. 157.

düşünülmektedir. Buna göre önleyici müdahale sadece ilk vuruşu yapabilmek için değil savaşı öne çekebilmek, erken bir savaş başlatmak istenildiği için de yapılabilmektedir.<sup>28</sup> Bu yüzdendir ki uluslararası hukukta tanımı ve meşruiyeti yoktur. Önleyici müdahale ile ilgili bir BM dayanağı olmaması nedeniyle, devlet dışı bir güvenlik tehdidi olan terörist grupların ve destekçilerinin ortadan kaldırılmasında Bush yönetimi önleyici müdahaleyi ön-alıcı müdahale olarak ele almıştır.<sup>29</sup> 2002 ABD UGS belgesi ABD'nin ulusal güvenlik için ön-alıcı müdahalenin emsalsiz bir durum olmadığını hatta gerekirse ABD'nin beklemeyip önleyici müdahale bile yapabileceğini, bunu kendinde hak olarak ele aldığını göstermektedir.<sup>30</sup> ABD'de Bush yönetimi böylelikle, ön-alıcı müdahalenin yanında terör gruplarını destek verdiği iddia ettiği devletlere karşı önleyici müdahaleyi de kullanacağını vurgulayarak artık toplu hareket eden uluslararası iş birliğinden vazgeçtiğini göstermiştir.<sup>31</sup>

Bush yönetimi önleyici müdahalenin ABD kamuoyunda meşru müdafaa olarak görünmeyebileceğini düşünmüştür. Amerikalılar ABD'nin Soğuk Savaş'ın caydırıcılık ve çevreleme politikasından ayrıldığına ve taarruza geçtiğine inanacaklardı. Bu açıdan önleyici müdahale kavramına ön-alıcı müdahale kavramı gibi davranarak kendini savunma algısı kamuoyunda bir haklı sebep yaratmıştır.<sup>32</sup> Kaldı ki hegemonyanın dünya istikrarı için ve barışın sağlayıcısı olduğu için gerekli görülen yeni-muhafazakâr anlayış yani Bush yönetiminin hâkim olduğu anlayış, şartların gerekli olması durumunda ABD'nin hegemonya vasfına layık olarak ön-alıcı müdahalede bulunabileceğini savunmaktadır.<sup>33</sup>

2002'de Başkan Bush, ön-alıcı ve önleyici müdahale kavramlarının önce West Point'deki Askerî Akademisi'ndeki konuşmasıyla ABD politikasının

---

<sup>28</sup> Karl P. Mueller vd., *Striking First*, s. 8.

<sup>29</sup> Kegley, Charles W. ve Gregory A. Raymond. "Preventive War and Permissive Normative Order." *International Studies Perspectives*, 4:4, 2003, s. 386.

<sup>30</sup> The USA National Security Council "The National Security Strategy September 2002 Chapter V. Prevent Our Enemies from Threatening Us, Our Allies, and Our Friends with Weapons of Mass Destruction" <https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/nss5.html>

<sup>31</sup> Stephen Van Evera, "A Farewell to Geopolitics", Eds.: Melvyn P. Leffler ve Jeffrey W. Legro, *To Lead The World: American Strategy after the Bush Doctrine*, Oxford University Press, Oxford ve New York, 2008, s. 18.

<sup>32</sup> Flynn et al., *First strike*, s. 220.

<sup>33</sup> Brian C. Schmidt ve Michael C. Williams, "The Bush Doctrine and the Iraq War: Neoconservatives Versus Realists", *Security Studies*,17, 2008 s. 198.

dayanakları olacağını göstermiş, ardından aynı yıl Bush Doktrini'nin 2002'de açıklanmasıyla doktrin dayanağı olarak kullanmıştır. Böylelikle önleyici müdahale ön-alıcı müdahale ile ilişkilendirilmiştir.<sup>34</sup> Bu açıdan bu kavramlarla ilk vuruş hakkı üzerine kurulu bir Doktrin oluşmuş ve kuvvet kullanımında gerekirse tek başına hareket edilebileceği savunulmuştur. Önleyici müdahaleyi destekleyen Bush Doktrini sakıncalı bulunduğu rejimleri değiştirmek için güç kullanımını müttefiklerin tavsiyelerini dikkate almadan dahi yapabileceğini savunmuştur.<sup>35</sup> Terör gruplarının saldırmasını beklemeden onlara karşı ilk vuruşu yaparak böylesi bir tehdidi ortadan kaldırmak aktif bir ABD politikasının göstergesi olmuştur.

Ön-alıcı müdahalenin fiziksel kanıtları sınıra asker yığmak ve hatta gelişen teknoloji ile uydu görüntüleri üzerinden olası saldırı verilerine ulaşabilmek üzerinden sağlanabilir. Diğer yandan modern teknoloji düşman unsurların gizlenebilmelerini de kolaylaştırmıştır. Teröristlerin eylemlerinin gizlenebilmesinde gelişen teknolojinin de payı vardır. Gelişen teknoloji artık gerek terörist eylemlerinin oluşum sürecindeki tespit zorluğu gerekse devletlerin örneğin sınıra askerî yığınak yapabilmekteki hızı ön-alıcı müdahale kararı için hızlı bir karar sürecini gerektirebilir. Ancak yine teknoloji sayesinde aynı silahlarla düşman unsurların belirlenmesi durumunda ön-alıcı müdahale dayanağı ortaya çıkabilmektedir. Hatta bu konuda ABD eski Dışişleri Bakanı Henry Kissinger eğer ki terörist karargâhlarının ve kamplarının bulunduğu ülkeler tespit edilebilirse bunun ön-alıcı müdahale için kuvvet kullanılmasında bir meşru dayanak olduğunu ileri sürmektedir.<sup>36</sup>

Gelişen teknolojinin dijital alan örnekleri bu konuda daha kapsamlı ve karmaşık bir alanı doğurmuştur. Teknolojik gelişmeler olası saldırıların keşfedilmesinde kolaylık sağlarken diğer yandan olası saldırıların matematiksel olarak gerçekleşme ihtimalleri de yapılmaya başlanmıştır. Peki, gerçek dünyanın taklitleri olarak simülasyonlar üzerinde yaratılan dünyalarda gerçekleşen olasılıkların matematiksel verileri gerçek dünyada devletlerin kararlarını nasıl etkilemelidir? Simülasyon uygulamasından elde edilen bir

---

<sup>34</sup> Thomas Donnelly, *The Military We Need The Defense Requirements of the Bush Doctrine*, The AEI Press, Washington, 2005, s. 87

<sup>35</sup> Stanley A. Renshon, *National Security in the Obama Administration Reassessing the Bush Doctrine*, Routledge, New York 2010, s. 22

<sup>36</sup> Henry Kissinger, Preemption and the End of Westphalia, *New Perspectives Quarterly*, 19:4, 2002, s. 31-36.

ülkenin bir ülkeye saldırma durumu yüzde 50'nin üstündeyse bu ön-alıcı müdahale olarak kullanılabilir mi? Düşman veya rakip devletlerin fiziksel güç verileri üzerinden yaratılan simülasyonların ortaya çıkardığı sonuçlar savaş sebebi olarak gösterilebilir mi? İşte dijital alanın hayatımıza girmesiyle uluslararası hukuk alanındaki boşluklar büyük bir tartışmayı yaratmış olmasına ek olarak devletlerin böylesi bir dayanak ile dış politikalarını dijital verilere göre yürütmeleri meselesi de eklenmiştir.

## 2. Dijital Alanda Güç: Simülasyonlar ve Ön-alıcı Müdahale

Devletlerin gerek diplomasi kabiliyetlerini geliştirmelerinde gerekse uluslararası anlamda güç elde etmelerinde dijital yetenekler belirleyici olmaya başlamıştır. Teknolojik gelişmişlik seviyesi ülkelerin üstünlüklerinde önemli bir zorunluluk haline gelmiştir. Çünkü dijital kabiliyetler devletlerin güç yeterliliklerinde belirleyici unsurlar arasına girmiştir. Örneğin askerî anlamda savaş araçlarının teknolojik alt yapı bakımından diğer devletlere göre üstün olması, savunma sistemi yazılımlarının ileri teknoloji veya millî tasarımlar olması devletlerarası rekabette belirleyici olabilen dijital gelişmişliklerdir.

İnternetin hayatımıza girmesi askerî anlamda bir ihtiyaçtan doğmuştur. İlk olarak ABD Savunma Bakanlığına bağlı ARPA ile oluşturulmuş, ARPANET adı verilen ağ askerî iletişim projesinden çıkıp tüm dünyaya ve sektöre yayılmıştır.<sup>37</sup> Böylelikle internet ve internet ile bağlantılı bulut bilişim, simülasyon veya yapay zekâ gibi yeni kavramların da içinde olduğu bilgiye dayalı bir dijital çağ ortaya çıkmıştır.

Devletler askerî kurumlarını dijital tabanlı uygulamalara adapte etmeye zorlamaktadır. En basitinden insansız hava araçlarının üstünlükte önemli bir etken olması söz konusuysen bunların millî tasarımlar olması hatta yapay zekâ ile desteklenmesi güç bakımından giderek daha çok belirleyici olan gelişmeler olmaktadır. Diğer yandan siyasi ilişkiler bakımından da dijital gelişmelerin adaptasyonu gerekli görülmektedir. Dışişleri Bakanlıkları dijital uygulamaları bu doğrultuda diplomasi sürecinde ya da yabancı halkların belirli konularda kendi iradeleri ile ikna edilebilmesi süreci olan kamu diplomasisi gibi yumuşak güç yöntemleri için kullanmaktadırlar. Bu açıdan dijital uygulamalar dış politikada belirleyici olmaya başlamıştır. Ayrıca üstünlük bakımından kullanılan dijital alanın uluslararası krizlere de konu

---

<sup>37</sup> National Research Council, *The Changing Nature of Telecommunications/ Information Infrastructure*, The National Academies Press, Washington, 1995, s.183.

olması önemini göstermektedir. Dijital diplomasi, siber savaş, siber saldırı gibi kavramların uluslararası ilişkilere girmesi ile gündemde öne çıkan Wikileaks krizi, Snowden olayı, Bitcoin krizi veya Anymous siber korsan saldırıları gibi dijital krizler devletleri zora sokar bir hal almıştır.

Dijital alandaki devletlerin önemli bir rekabet konusu da yapay zekadır. Yapay zekânın savaşta kullanılabilirliği üzerine bir endişe söz konusudur. Yapay zekâ konusunda rekabete giren devletler yapay zekâ tasarımlarına insansı özellik kazandırmak için mücadele etmektedirler. Vatandaşlık vermek, belirli meslek gruplarında insan görünümü yapay zekâlar üretmek gibi girişimlerde bulunmuşlardır. Dolayısıyla küresel rekabet için devletler yapay zekâ konulu büyük yatırımlar ve projeler odağında ilerlemektedir. Örneğin Çin, yapay zekâ konusunda lider olabilmek için kendisine “Made in China 2025” adında bir proje hedefi koymuştur.<sup>38</sup>

Güvenlik alanında yapay zekâ ile desteklenmiş tasarımların oluşturulması giderek artmaktadır. Yapay zekâ destekli simülasyonlar bu etkili üstünlük dayanaklarında devletlerin artık başvurdukları konulardandır. Simülasyonlar üzerinden bürokratik eğitimler veya olasılık hesapları devlet karar alıcıları için başvuru konular arasına girmiştir. Dijital alan devletlerin politik eylemlerinde artık belirleyici olmuştur. Bu noktada dijital alanda yaratılan simülasyonlar devlet kurumlarında kullanılan önemli alanlardan olmuştur. Simülasyonlar, artırılmış gerçeklik ortamları veya sanal dünyalar gerçek dünyadan bağımsız olmamaktadır.

Simülasyon gerçek dünyanın matematiksek olarak modellenmesi ile oluşan sanal dünyadır. Simülasyon teknik olarak bilgisayarlarda 0 ve 1’den oluşan rastgele sayıların değişken aralıklarla bir arada bir dizi oluşturulmasıyla tasarlanır. Simülasyonların faydalı olacağı ve kullanılacağı belli başlı konular vardır. En nihayetinde bir hipotezin test edilmesinde kullanılır. Diğer yandan sosyal hayatı düzene sokmak için, örneğin bir hastanede hasta akışını modellemede, bir salgının evriminin modellenmesi ve finansal alanda fiyatlandırmalarda kullanılan modellemelerde kullanılabilir.<sup>39</sup>

---

<sup>38</sup> Institute for Security & Development Policy, “Made in China 2025 Backgrounder” June 2018, <https://isd.dp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf>, erişim 11.05.2023.

<sup>39</sup> Juhn S. Dagpunar, *Simulation and Monte Carlo With applications in finance and MCMC*, John Wiley and Sons, Chichester, 2007, s. 1.

Simülasyonlarda gerçek hayattaki durum modellenir veya benzer bir dünya yaratılır. Bunun için tamamen analitik yöntemler kullanılır. Teknik bir ifade ile çözümü zor çoklu bir integrali tahmin edebilir çözümler üretmektedir. Bununla ilgili 1940 yılından kalma yöntemler halen daha kullanılmaktadır. Monte Carlo yöntemi simülasyon oluşturmanın ve istatistiksel çıkarımlar yapabilmeyen en güzel klasik örneğidir.<sup>40</sup>

Monte Carlo simülasyonu John von Neumann ve Stanislaw Ulam tarafından 1940'larda icat edilir. Rulet oyunu gibi rastgelelikten ilham alınan simülasyon tasarımı bu yüzden Monako'daki bir kumarhanenin ismini alır. Simülasyona göre farklı olasılıklar oluşturulur ve her biri farklı sonuçlar doğurur. Örneğin finans sektöründe risk analizi yapmak için karar alıcılıkta gerçekçi senaryolar oluşturulur. Hisse senedi fiyatları konusunda tavsiyeler oluşturmak için de benzer şekilde piyasada olası sonuçlar oluşturulur.<sup>41</sup>

Makine öğrenimi ile simülasyonlar arasından temelde farklılık vardır. Makine öğrenimi yapay zekâ konusudur. Makine öğrenimi ile tüketilen verilere göre performans iyileştirilir. Yapay zekâ ise insan zekasını taklit eden daha genel sistemlerdir. Makine öğrenimi bu yapay zekâ sistemlerinden biridir. Makine öğrenimi iyileştirme yapabilmek için simülasyonları kullanabilir.<sup>42</sup>

Yapay zekâ destekli teknolojileri bir güç unsuru olarak kullanabilmek önemli bir rekabet konusu olmaktadır. Özellikle Uluslararası ilişkiler alanında güvenlik konusunda kullanılabilir olması yapay zekâ ve yatırımlarını arttırmaktadır. Bu da küresel teknoloji şirketlerinin devletlerle olan ilişkilerinin artmasına neden olmaktadır. Uluslararası etkisi olan aktörler tanımlanmasına ulus aşırı şirketlerin de girdiğine yönelik tartışmaların kaynağı da bundandır.

Devletler gelecek politikalarının yol haritalarını belirlemek için kamuoyu verilerine erişmek istemekte, bu yüzden iletişim teknolojileri alanındaki büyük şirketlerle görüşme yapmaktadır. Diğer yandan bazı devletler savunma konusunda kendini güçlendirmek için savunma sanayi alanında olan şirketlerle bağ kurmaktadır. Bazı devletler ise yapay zekâ konusunda faydalar sağlamak için yapay zekâ şirketleri ile anlaşmalar yapmaktadır.

---

<sup>40</sup> Amazon, "Monte Carlo Simülasyonu nedir?", <https://aws.amazon.com/tr/what-is/monte-carlo-simulation/>, erişim 11.05.2023.

<sup>41</sup> Amazon, "Monte Carlo Simülasyonu nedir?"

<sup>42</sup> Microsoft, "Makine öğretiminde ve pekiştirici öğrenmede konu uzmanlığını kullanma", <https://learn.microsoft.com/tr-tr/azure/architecture/solution-ideas/articles/machine-teaching>, erişim 11.05.2023.

Simülasyonları uluslararası ilişkiler alanında kullanan devletlerin sayısı her geçen gün artmaktadır. Bu süreç aslında sanal gerçeklik projeleri ile başlamaktadır. Sanal gerçeklik ile gerçek dünya deneyimlerini sanal ortamda yineleyerek simülasyonların oluşturulması için veri elde edilebilir. Sanal gerçeklikte belirli bir senaryo gerçek dünya deneyimleri ile aktarılır. Yani gerçekçi deneyimler senaryolaştırılır.<sup>43</sup> Simülasyonlarda ise gerçek dünyanın verileri girilerek gerçek dünya için olasılıklar hesaplanabilir.

Sanal dünya ortamını uluslararası ilişkiler adına kullanan devletlere örnek olarak İsveç ve Maldivler gösterilebilir. Bu iki ülkenin çalıştığı şirket Linden Lab şirketidir. İsveç sanal dünyada büyükelçilik açan ilk ülkedir.<sup>44</sup> Bu şirketin tasarladığı 2007 yılındaki proje *Second Life* adında bir simülasyondur.<sup>45</sup> Bu sanal dünya inşasındaki katılımcılar gerçek dünyadaki aktörler gibi davranmakta ve devlet ilişkileri gerçek hayatta nasıl ise orada da benzer şekilde eylemler yapmaktadır. Hatta *Second Life* sakinlerinin kullandığı para birimi Linden'dır.<sup>46</sup> Gerçek dünyadaki devletler dışında şirketlerin de bu sanal dünyada temsilcilikleri vardır. Proje devam etmemekte ancak veri elde etme ve tecrübe edinme bakımından değerli örneklerdendir.

Gerçek hayatta olan devlet kurumlarının sanal varlıkları yukarıdaki örnekteki gibiyken gerçek hayatta var olamayan kurumlar dijital ortamlarda varlık göstermeye başlamıştır. Örneğin İran Büyükelçiliği sadece sanal ortamda oluşturulmuştur.<sup>47</sup> ABD-İran ilişkilerinin bozulmasından itibaren kapalı olan ABD'nin İran Büyükelçiliği web sayfası üzerinden bir dijital varlık göstererek yeniden açılmıştır. ABD ile ilişkileri iyi olmayan İran, sürekli bu sanal elçiliğe siber saldırıda bulunsa da, buna karşılık ABD ise ısrarla bu büyükelçiliğini yeni ağ uzantısından tekrar açmıştır. Bu büyükelçilik gerçek dünyada fiziksel büyükelçilik imkânı olunmamasından dolayı dijital platformlardan elçilik görevinin yürütüldüğü bir alandır. Bu anlayışta hem sanal gerçeklikten hem simülasyondan ayrılmaktadır.

---

<sup>43</sup> Dilan Ezgi Düzgün, Yudum Kayhan, Kerim Çetinkaya, *Simülasyondan Artırılmış Gerçekliğe*, 4th International Congress on 3D Printing, Technologies and Digital Industry, 11-14 Nisan 2019, Antalya.

<sup>44</sup>Reuters, "Sweden first to open embassy in Second Life", <https://www.reuters.com/article/us-sweden-secondlife-idUSL3034889320070530>, erişim 11.05.2023.

<sup>45</sup> Secondlife, <https://secondlife.com/>, erişim 11.05.2023.

<sup>46</sup>Linden Lab, "About Linden Lab", <https://www.lindenlab.com/>, erişim 11.05.2023.

<sup>47</sup> US Virtual Embassy Iran, <https://ir.usembassy.gov/>, erişim 29.06.2023.

Diplomasıde teknoloji o denli önemli olmuştur ki devletler teknoloji şirketleri ile bir devletmiş gibi temas kurmaya başlamıştır. Bu teknoloji devleri devletlerin karar süreçlerinde önemli aktörler olmaya başlamışlardır. Uluslararası hukuk anlamında bir devletin başka devlet toprağı sınırlarındaki temsilciliğı olan büyükelçilikler veya konsolosluklar artık teknoloji devleri için de oluşturulmaya başlanmıştır. Örneğın Silikon Vadisi için 2017’de kurulan büyükelçilikler vardır. Danimarka Silikon Vadisi Büyükelçiliğı bu konuda ilktir.<sup>48</sup>

Devletler Apple, Facebook, Google, Microsoft gibi şirketlerle önemli projelere girişmektedir. Kurumların dijital dönüşümlerinde devletlerin bu gibi önemli şirketlere ihtiyacı vardır. ABD’nin bu dönüşümde ve teknolojinin politika ile birleşmesinde atılımcı yapısı burada kendini göstermektedir. Örneğın ABD Dışışleri Bakanlığı Microsoft ile yapmış olduğı proje kapsamında diploması konusunda sanal eğitimler vermektedir. 2015 yılında başlatılan projedeki yer alan konulardan biri *Surface Hub* yani beyaz tahta teknolojisi ile diplomatların yetenekleri geliştirilip karar verme yetisinde başarılı sonuçlar ortaya çıkarabilmek için simülasyonların oluşturulmasıdır.<sup>49</sup>

ABD diploması merkezinin Microsoft ile yaptığı anlaşmalarda teknoloji ile desteklenen diploması eğitimlerinde farklı birçok simülasyon oluşturulmaktadır.<sup>50</sup> “*Gamifying diplomacy*” denilen gerçek dünyanın taklit edilmiş versiyonu olan simülasyon diploması oluşturulmaktadır.<sup>51</sup> Örneğın 1898 İspanya-ABD Savaşı: anlaşmalar ve kendi kaderini tayin hakkı veya Süveyş Kanalı krizi gibi tarih temalı simülasyon, uluslararası göç krizi, tatlı su krizi: enerji güvenliğı ve ekonomik büyüme temalı veya sınır güvenliğı: çatışma çözümü ve önleyici diploması temalı farklı birçok eğitici ve yetenek geliştirici diploması simülasyonu geliştirilmiştir.<sup>52</sup> Bu dijital ortamda,

---

<sup>48</sup> Ministry of Foreign Affairs of Denmark, “The TechPlomacy Approach”, <https://techamb.um.dk/the-techplomacy-approach>, erişim 11.05.2023.

<sup>49</sup> Microsoft, “Surface Hub 2S”, <https://www.microsoft.com/en-us/surface/business/surface-hub-2>, erişim 11.05.2023.; Microsoft, “Diplomacy Everywhere: Microsoft donates cutting-edge technology to bring diplomacy to life for visitors of the U.S. Diplomacy Center”, <https://blogs.microsoft.com/on-the-issues/2015/02/25/diplomacy-everywhere-microsoft-donates-cutting-edge-technology-to-bring-diplomacy-to-life-for-visitors-of-the-u-s-diplomacy-center/>, erişim 11.05.2023.

<sup>50</sup> The National Museum of American Diplomacy, “Diplomacy Simulations: Immerse students in the world of American Diplomacy”, <https://diplomacy.state.gov/education/diplomacy-simulations/>, erişim 11.05.2023.

<sup>51</sup> Microsoft, “Diplomacy Everywhere”.

<sup>52</sup> The National Museum of American Diplomacy, “Diplomacy Simulation”, <https://diplomacy.state.gov/education/diplomacy-simulations/>, erişim 11.05.2023.



gerçek dünyada oluşan krizlerde veya diplomasi pazarlığında alınabilecek kararlar nasıl ise aynı şekilde kararlar alınıp başarı testi yapılmaktadır.

Simülasyon teknolojisi eğitimde ve yetenek geliştirmede kullanılan bir destek etkeni iken diğer yandan savaş konusunda savunma sanayisinde kullanılmaktadır. Savaş olasılıklarının hesabı devletlerin karar almalarında en zor süreçler olarak yorumlanabilir. Bu tür karar alma süreçlerinde yapay zekâ destekli yanılma payını indirgeyici dayanaklara başvurmak giderek tercih edilir bir durum olmaktadır. Türkiye bu konuda savunma sanayisini yapay zekâ ile birleştirmeye çalışan ülkeler arasındadır. Hatta öğrenen yapay zekâ ile makine öğreniminden de faydalanarak projeler geliştirilmektedir. Makine öğrenimi, yapay zekâ ve simülasyon teknolojisi böylelikle birleştirilmektedir. Örneğin Havelsan 2020 yılında Yapay Zekâya Sahip Sanal Kuvvetler (FIVE-ML) ARGE projesini başlatmıştır. Projeyi Havelsan'ın Eğitim ve Simülasyon Teknolojileri birimi yürütmektedir. Böylelikle taktik eğitim verilmesi, senaryo planlaması, gerçek ortamlarda kullanılacak karar süreçlerinin geliştirilmesi hedeflenmiştir.<sup>53</sup>

Simülasyonların askerî birimlerde kullanılabilirliği ABD ordusunda kullanılmak için yeni teknolojiler geliştirmekten sorumlu DARPA'nın çalışmalarında da yer almaktadır. Bilindiği üzere DARPA internetin icat edilmesinde rol alan kurumdur. DARPA'nın geliştirdiği ulusal siber saha (*national cyber range*) programı simülasyonları silahlı kuvvetlerin siber savaş yeteneklerini geliştirmek için de kullanılmaktadır.<sup>54</sup> Tahmine dayalı operasyonel çıktılar oluşturmak için simülasyonlar tercih edilmektedir. Ayrıca maliyet, pratiklik ve en önemlisi de gerçek dünya seçimleri için bu simülasyonlar işlevseldir.<sup>55</sup> ABD, ordusu için simülasyon eğitiminden yararlanan devletlerdendir. ABD ordusunun üç tür simülasyon eğitimi vardır. Bunlar sanal gerçeklik uygulama eğitimi, gelişmiş dağıtılmış etkileşim ve sanal gerçeklik kombine uygulama eğitimidir.<sup>56</sup>

---

<sup>53</sup> Havelsan, "Havelsan Yapay Zekâli Simülâtör Geliştirecek", <https://www.havelsan.com.tr/haberler/guncel/havelsan-yapay-zekali-simulator-gelistirecek>, erişim 11.05.2023.

<sup>54</sup> The USA the Department of Defense "National Cyber Range", <https://www.peostri.army.mil/national-cyber-range-ncr>, erişim 11.05.2023.

<sup>55</sup> The USA National Initiative for Cybersecurity Education, "The Cyber Range: A Guide: Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training" [https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420\\_1315.pdf](https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf), erişim 11.05.2023.

<sup>56</sup> Kai Yao ve Shaoluo Huang, "Simulation Technology and Analysis of Military Simulation Training", *2021 Journal of Physics: Conference Series*, 1746, s. 2

Simülasyon tasarımları yapabilen teknoloji şirketleri bir sektörü oluşturmaktadır. Nasıl ki siber güvenliğin ulusal güvenliğin bir parçası haline gelmesiyle ve devletlerin güvenlik tedbirlerinde bir zorunluluk olmasıyla uluslararası siber güvenlik şirketlerinin sayısının ve öneminin artması söz konusu olduysa, benzer şekilde simülasyonların dış politikadaki karar alma süreçlerine ve güvenlik tedbirlerine katkısı göz ardı edilememiş ve simülasyon tasarımları yapan şirketlerin sayısı her geçen gün artmıştır. FAAC bu simülasyon sağlayıcı şirketlerdendir. Üniversitelerin orduları destekleyici projeleri de bu yönde etki yaratmaktadır. ABD ordusu akademisi olan West Point Askerî Okulu'nun Simülasyon Merkezi de bu anlamda askerî simülasyonların geliştirilmesinde katkı sunmaktadır.<sup>57</sup>

Princeton Üniversitesi'nin benzer şekilde savaş simülasyonları oluşturmakla ilgili projeleri vardır. Örneğin, Nükleer Savaş Simülatörü ABD ile Rusya arasındaki bir nükleer savaş olasılığını inceler. Kıtalar arası balistik füzelerin varlığı veya yokluğu üzerinden simüle edilmiş bir veri sunmaktadır. Simülasyon, nükleer silah patlaması, ısı, yangın ve radyasyon etkilerini ortaya koymaktadır. Ölümleri, askerî hedeflere saldırıları tahmin ederek gerçek hayattaki karar almaya etkisini ortaya koymaktadır.<sup>58</sup> Simülasyonun Plan A denilen sonucuna göre ABD ve Rusya arasındaki çatışmanın ilk birkaç saatinde 90 milyon insan ölüm ve yaralanma ile etkilenecektir.<sup>59</sup>

Simülasyonlar uluslararası askerî konularda uluslararası iş birliklerinde de kullanılmaktadır. Hatta büyük boyutlu projeler için sadece bilgisayar üzerinde sınırlı olmayabilir. Bunun için Asya'da gerçekleştirilen simülasyon tatbikatı örnek verilebilir. Hem boyutu büyük hem de katılımların birden fazla olması bakımından farklıdır. Güney Kore'de düzenlenen Key Resolve veya Foal Eagle diğer yandan Japon kuvvetleri ile düzenlenen Keen Edge ve Tayland'da düzenlenen Cobra Gold büyük ölçekli tatbikatlardır. Bunlar bilgisayar simülasyonları ile etkileşime geçilerek birleştirilmiş sistemlerdir. Böylelikle gerçek kuvvetlerle simülasyon sistemleri birleşmiştir.<sup>60</sup>

---

<sup>57</sup>The United States Military Academy, "West Point Simulation Center", <https://www.westpoint.edu/military/department-of-military-instruction/simulation-center>, erişim 11.05.2023

<sup>58</sup> Princeton University, "Simulating Nuclear War", <https://sgs.princeton.edu/the-lab/simulating-nuclear-war>, erişim 11.05.2023.

<sup>59</sup> Princeton University, "Plan A", <https://sgs.princeton.edu/the-lab/plan-a>, erişim 11.05.2023

<sup>60</sup> Raymond R. Hill J. O. Miller, A History of United States Military Simulation, Proceedings of the 2017 Winter Simulation Conference, s. 347.

Simülasyonların askerî güvenlik konularında ve küresel krizlerde kullanılabilirliği Rusya'nın saldırgan politikaları için de görülmektedir. Simülasyon sistemleri Rusya'nın yayılmacı ve saldırgan politikalarına karşın devletlerin güvenlik garantileri almaları için güvenlik endişelerini kanıtlayıcı matematiksel hesaplamalar yapmalarında bir seçenek olmuştur.

ABD'nin askerî eğitim üniversitelerinden biri olan Deniz Piyadeleri Üniversitesi (*Marine Corps University*) savaş oyunlarının, simüle edilmiş ortamda askerî yetenekleri geliştireceği gerekçesiyle eğitim sistemine alınmasını uygun görmüştür. Savaş oyunu eğitimi için bir rapor hazırlanmıştır. Buna göre savaş oyunlarının kriz yönetiminde önemli kararlar alınması için eğitici ve öğretici olduğu vurgulanmıştır. Böylelikle ABD Ordu Komutanlığı ve Genelkurmay Koleji'nde simülasyon üzerindeki savaş oyunlarının kullanılmasının birçok farklı derste uygun olduğu vurgulanmıştır.<sup>61</sup>

Deniz Piyadeleri Üniversitesi savaş senaryoları üzerinden veri elde etmek isteyen projeler de yapmıştır. Bir üçüncü dünya savaşı olursa ABD'nin kazanma olasılığının hesaplanması ve savaşın seyri için bir proje hazırlanmıştır. Bu simülasyona göre Rusya Baltık Ülkeleri'ni ve Ukrayna'yı ele geçirmektedir. Daha sonra Rusya Polonya'yı tehdit etmiştir. Diğer yandan Çin de Rusya'nın dikkatleri kendine çekmesinden faydalanarak Tayvan'ı ele geçirme girişimlerinde bulunmaktadır. Rusya ve NATO'nun savaşında deniz, hava, kara harekât olasılıkları için askerî birliklerin sayı ve konumları dahi detaylı simüle edilmiş bir oyunda canlandırılmıştır.<sup>62</sup> Buna benzer savaş senaryosunu simüle eden ve Rusya'nın saldırması durumundaki olasılıkları hesaplayan bir başka simülasyon Polonya Savaş Çalışmaları akademisidir (*the Polish War Studies Academy*). Zima adlı simülasyon resmî olarak duyurulan bir proje olmamasına rağmen basına sızmasından dolayı duyurulmuş bir projedir. Sızan bilgileri Polonya devlet yetkilileri yalanlamamıştır.

Zima 2020 (Kış 2020) adlı simülasyon operasyonu Rus saldırısının hesaplanması için tasarlanmıştır. 2020 yılında hazırlanan simülasyon henüz Ukrayna Savaşı başlamadan önce hazırlanmıştır. Simülasyona göre Rus saldırısı olursa Polonya'nın bir Rus saldırısından korunması için direnme

---

<sup>61</sup> Sebastian J. Bae (Ed.), *Forging Wargamers: A Framework for Wargaming Educations*, Marine Corps University Press, 2022, Quantico s. viii

<sup>62</sup> James Lacey, "How Does The Next Great Power Conflict Play Out? Lessons From A Wargame", *War on the Rock*, April 22, 2019, <https://warontherocks.com/2019/04/how-does-the-next-great-power-conflict-play-out-lessons-from-a-wargame/>, erişim 11.05.2023.

süreci hesaplanmak istenmiştir. Rus tanklarının işgal yeteneği üzerinden bir simülasyon hazırlanmıştır. Gizli yapılan bu simülasyonun sonuçlarının da gizli kalması gerekirken Interia ve Onet gibi bazı haber sitelerine sızmıştır. Ayrıca, simülasyon sonucuna göre beklenmeyen bir netice çıkmıştır. Buna göre Ruslar dört gün içinde Polonya'yı işgal edebilecektir. Bu sonuç Polonya'nın savunma açıkları hakkında bir öngörü sağlamaktadır. NATO'nun desteği, 140 bin Polonyalı askerin ve ABD uçak savar sisteminin olmasına rağmen böylesine bir sonuç çıkmıştır.<sup>63</sup> Bu tür matematiksel verileri dayanak olarak göstererek Polonya'nın NATO'dan daha fazla destek istediği iddiaları da yapılmaktadır. Çünkü bu tür simülasyon verileri devlet karar alıcılığında giderek dayanak olarak kullanılmaya başlamıştır. Diğer yandan bu sızdırılmanın simülasyon verilerinin doğruluk payını değiştirmeyeceğinin de altı çizilerek ciddiye alınması ve Rusya'ya karşı tedbir alınması gerektiğini vurgulanmaktadır.

Rusya'nın yayılcı bir politika izleyerek özellikle Baltık Ülkelerinin kıyılarına asker yığması, tatbikatlar yapması, Polonya ve Ukrayna gibi devletleri simülasyon verilerinden yararlanmaya itmiştir. Zaten 24 Şubat 2022'de Rusya'nın Ukrayna'da başlattığı illegal işgali bu endişeleri haklı çıkarmıştır. Bu noktada Zima gibi programlar olasılık ve matematiksel hesaplamalar ile devletlerin güvenlik risk oranlarını göstermeleri ve tedbir almaları bakımından bir dayanak olarak kullanılabilir hal almaya başlamaktadır.

Akademik çalışmalarda, üniversitelerde, orduda veya harp okullarının eğitimlerinde görülmektedir ki simülasyonun dış politika analizinde bir etkisi vardır. Zaten simülasyonun askerî politikalar bakımından amacı savaş planlaması, savaş zamanı operasyonları, tedarik, kuvvet boyutlandırma, insan kaynakları planlaması, lojistik ve konuşlandırma planlaması gibi ulusal güvenliği destekleyici unsurlardır.<sup>64</sup> Ancak tüm bunların genelini kapsayan asıl amaç genel bir ulusal politika analizi yapabilmek ve bunu da olabildiğince hatasız yapabilmektir.

---

<sup>63</sup> Hüseyin Koyuncu, "Askeri Simülasyon Basına Sızdı: Rus Ordusu Varşova'yı 4 Günde Kuşatabilir", <https://tr.euronews.com/2021/02/06/rus-ordusu-polonya-ya-sald-r-rsa-baskent-varsova-sadece-dort-gunde-kusat-l-r>, erişim 11.05.2023.

<sup>64</sup> John A. Battilega ve Judith K. Grange, *The Military Applications of Modeling*, Air Force Institute of Technology Press, Ohio, 1984, s. 7; Raymond R. Hill ve John O. Miller, "A History of United States Military Simulation", *Proceedings of the 2017 Winter Simulation Conference*, s. 198.

## Sonuç ve Tartışma

Devletler için diğer aktörü düşman olarak isimlendirmek korkuların tanımlanmasıyla yapılan, duygu ve sezgilerin de etkili olduğu bir durumdur. Bu uluslararası ilişkilerin anarşik yapısında doğal görülen bir devlet davranışı olarak yorumlanabilir. Ancak devletler, güvenlik endişelerinin kaynağı olan karşılıklı korkularını meşru müdafaa olarak görünen bir müdahale yapacak oranda geliştirmek için bilimsel kaynaklara başvurmayı giderek tercih edilir yapmaktadırlar. Somut ve korku kaynağını meşrulaştıracak verileri öne sürerek bunu yapmak uluslararası anlamda daha fazla toplumsal desteği almaya neden olacaktır.

Devletlerin korkularını meşrulaştıracak dayanaklar diğer aktörlerce eleştirilebilir. Bir devletin tehdit algılaması durumunda kendini güvenceye alması gerekirken, bu da ön-alıcı ve önleyici müdahalelerle yapılmaktadır. Bunun için de tehdidin varlığı ile ilgili kanıtlara ihtiyaç duyulmaktadır. Devletler bu tür kanıtlar için geçmişten, günümüzden, toplumsal yapıdan ve benzeri birçok dayanaktan kanıtlar sunmaya, istihbarat edinmeye başlar. Simülasyon verileri bu tehdit analizleri için kullanılmaya başlayan önemli gelişmeler olmaktadır. Simülasyon verileri ön-alıcı müdahale yapılabilmesi için bir tehdit kanıtı olarak görülmeye başlamaktadır. Çünkü teknolojik gelişmeler ilerledikçe bu dayanaklar çeşitlenmektedir. Beşerî kararlardan bağımsız bir matematiksel veri topluluğu olan kanıtlar daha fazla meşrulaştırma sağlayacağından daha güvenilir sonuç verebilmektedir.

Matematiksel olasılık hesaplamalarının uluslararası ilişkiler anlamında ne derece devletleri ilk vuruş seçeneğine götürmede güvenilir ve destekleyici olduğu yine de belirgin değildir. Gününüz bu sürecin geçiş evresindedir. Meşru müdafaa konularında çalışmanın ilk bölümünde de tartışıldığı gibi ön-alıcı bir meşru müdafaa belirli kanıtların gözle görülmesinden dolayı uygun bir seçenekken önleyici müdahalenin meşru bir dayanak olmasındaki ikna edici ve etik meselesi tartışmalıdır.

Simülasyon verileri ve yapay zekâ analizleri düşman tanımlaması ve saldırganlık göstergelerinin hesaplamalarında meşru bir hukuksal dayanak olup olmadığı uluslararası iş birliğinin şekli ve uluslararası aktörlerin kabul edilir seçenekleri meşrulaştırma süreçlerine göre değişmektedir. Yani ön-alıcı müdahale tanımında geçen gözle görülür tehdit tanımına uymasa da simülasyon verilerini devletlerin tehdit kanıtı olarak görmeye başladıkları söylenebilir. Örneğin ABD'nin Irak işgali konusunda önleyici müdahale yaklaşımını tartışmalı olsa da küresel manada destek alabilir seviyeye taşınması

söylemlerin yeri, zamanı, kullanımını ve iş birliklerinin şekli ile ilgili olmuştur. Yapay zekâ destekli simülasyon verilerinin de bir ön-alıcı dayanak olarak kullanılabilirliği uluslararası aktörlerin çıkarları gereği iş birliği ile sağladıkları ortak anlayışa bağlı olarak değişebilecektir.

Buna benzer şekilde aslından ön-alıcı bir müdahale kuralına uymayan sezgisel ve söylemsel tehdit tanımlamalarının dahi küresel aktörlerin yorumlamaları ve iş birliklerinin şekli itibari ile ön alıcı bir tedbirmiş gibi savaş hakkı olarak gösterilmesi mevcut uluslararası ilişkiler yapısında mümkün olaylardır. Bu sezgisel tehditlerin meşru müdafaa olarak kullanılmasına nazaran simülasyonlar ve yapay zekâ gibi matematiksel verilerin beşerî hatalardan arındırılmış sonuçları daha etkili bir dayanak olarak kullanılabilir. Zaten ön-alıcı müdahale doktrini ve önleyici müdahale doktrini arasında karmaşa olsa da, devletler makine düşünmesini, yapay zekâyı ve bilgisayar olasılık hesaplarını ön-alıcı müdahalede bir dayanakmış gibi yorumlayabilmektedir.

Uluslararası askerî güvenlik konusunda kullanımını giderek artan simülasyonların üreteceği veriler beşerî karar alma sürecine etki edeceğinden önemlidir. Makine hesaplamasının yanılma payı ile insan karar alıcılığının yanılma payı arasında devletlerin yaşamsal varlıklarını etkileyecek konular olması bakımından farklar vardır. Simülasyonlar, verilerinin doğruluk payının yüksekliği ile giderek daha güvenilir olması bakımından ihtiyaç haline gelmeye başlamıştır. Bu konu, yapay zekâ sisteminin mahkemelerde kullanılması gibi insani karar alınmasına nazaran makine kararının duygulardan arınmış ve mantıksal doğru kararlar için daha tercih edilir bir seçenek görülmesiyle benzerdir. Bu açıdan dış politikada devletlerarası rekabet ve özellikle savaş gibi yaşamsal sonuçlarının olabileceği kararlarda makine verilerine ve matematiksel hesaplamalara göre tercihler yapmak kararları daha meşrulaştırabilir ve de süreç ile ilgili tartışmalara daha savunulur bir boyut kazandırabilir. Bu açıdan dış politikada simülasyon verilerine göre karar almak geri plana atılmayacak bir seçenektir. Ancak şu da unutulmamalıdır ki matematiksel hesaplamalar ile uluslararası ilişkileri ilerletmek duygulardan arındırılmış ve diplomasinin pazarlık ihtimaline güvenmeyerek inancın zayıflamasıyla şiddeti körükleyen bir sonuçla da neticelenebilir.

## Summary

Thanks to simulations, probability calculations on important security issues of states have now become frequently used methods. However, the question remains: Can this security method tried to be provided with the digital space be a guiding factor as a basis of defence? Or should taking an action based on simulation data be interpreted as an attack? This study has undertaken to seek answers to these questions. The conceptual framework of the study is the concepts of pre-emptive and preventive intervention. In this context, the study discusses whether the use of simulation data as a basis of defence in interventions is a pre-emptive or preventive approach.

The study begins with the definition of the concepts of proactive and preventive intervention. Throughout history, resorting to war has been an important method in resolving international conflicts and disputes. The problem of using the concepts of pre-emptive and preventive intervention as a basis is complicated. Although there are differences between preventive intervention and pre-emptive intervention, there have been cases where they are used interchangeably due to conceptual confusion. Pre-emptive intervention is to prevent an attack by taking military action against an enemy. That is, one state launches a military attack on another after concluding that the other state in question is threatening to attack and cause great harm. Considered self-defence, this kind of attack is deemed justified and enshrined in international law. Preventive intervention, on the other hand, stems from the belief of the enemy due to heuristics and fear of security. Its existence is based on the belief of a possible enemy or attack that is not based on conclusive evidence. It seems preferable to feel safe by making the first hit rather than living with anxiety. Digital space examples of developing technologies have given birth to a more comprehensive and complex field in this regard. While technological developments facilitate the discovery of possible attacks, the possibility of possible attacks to occur mathematically has begun to be used, on the other hand.

The second part of the study emphasizes the interpretation of digital power in international relations and its importance and then gives examples and functions of simulations in this field. Digital capabilities have begun to be decisive in the development of the diplomacy capabilities of states and in gaining international power. The level of technological development has become an important necessity in the superiority of countries. In simulations, a real-life situation is modelled, or a similar world is created. Purely analytical methods are used for this. The number of states using simulations in the field of international

relations increases day by day. While simulation technology is a support factor used in education and skill development, it is also used in the defence industry for warfare. The calculation of war probabilities can be interpreted as the most difficult process for states to take decisions. In such a decision-making process, it is increasingly preferable to apply artificial intelligence-assisted bases that reduce the margin of error. Simulation has an impact on foreign policy analysis as the evidence from academic studies, universities and military education training shows.

As the conclusion and discussion part, the last part of the study discusses the usability of simulations as a basis in international relations. The legitimacy of using simulation data and artificial intelligence analyses for identifying enemies and calculating aggression indicators depends on the specific forms of international cooperation and the processes through which international actors establish acceptable options. Although the preventive war approach of the USA in Iraq intervention is controversial, it has brought global support to the level of the discourse, the use of time and the form of cooperation. Similarly, even the intuitive and discursive threat definitions which do not comply with the rule of pre-emptive intervention can be presented as a right to go to war as if they were pre-emptive measures through the interpretations of the global actors and the format of their cooperations within the current structure of international relations. Compared to the use of these heuristic threats as self-defence, the results of mathematical data such as simulations and artificial intelligence, which are free from human errors, can be used as a more effective basis. There is already confusion present between the doctrine of preventive warfare and the doctrine of pre-emptive war, and the states can and may interpret machine thinking, artificial intelligence, and computer probability calculations as a basis for pre-emptive intervention.

***Çatışma Beyanı:***

*Araştırmanın yazarları olarak herhangi bir çıkar çatışma beyanımız bulunmamaktadır.*

***Araştırmacıların Katkı Oranı Beyanı:***

*Yazarlar araştırmaya eşit oranda katkıda bulunmuştur.*



**Kaynakça****Başlı Eserler**

- AGIR Bülent Sarper (2006). “Bush Doktrini Küresel Bir Hegemonik İstikrar Arayışı mı?”, *Uluslararası İlişkiler*, 3:12, 71-100.
- BAE Sebastian J. (ed.) (2022). *Forging Wargamers: A Framework for Wargaming Educations*, Marine Corps University Press, Quantico.
- BATTILEGA John A. ve GRANGE Judith K. (1984). *The Military Applications of Modeling*, Air Force Institute of Technology Press, Ohio.
- BOUDREAU Donald G. (1993). “The Bombing of The Osirak Reactor” *International Journal on World Peace*, 10:2, 21-37.
- CHARTER OF THE UNITED NATIONS, Chapter I, Purposes and Principles Article 2(1)–(5), <https://legal.un.org/repertory/art2.shtml>.
- DAGPUNAR John S. (2007). *Simulation and Monte Carlo With applications in finance and MCMC*, John Wiley and Sons, Chichester.
- DONNELLY Thomas (2005). *The Military We Need The Defense Requirements of the Bush Doctrine*, The AEI Press, Washington.
- DÖNMEZ Suat (2017). “Kuvvet Kullanma Kapsamında Ön Alıcı ve Önleyici Saldırı Kavramları”, *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi*, 3:3, 8-15.
- DUNMİRE Patricia L. (2009). “9/11 Changed Everything: on Intertextual Analysis of the Bush Doctrine”, *Discourse & Society*, 20:2, 195-222.
- DUZGÜN Dilan Ezgi (11-14 Nisan 2019). Yudum Kayhan, Kerim Çetinkaya, *Simülasyondan Artırılmış Gerçekliğe*, 4th International Congress on 3D Printing, Technologies and Digital Industry, Antalya.
- EVERA Stephen Van (2008). “A Farewell to Geopolitics”, Eds.: Melvyn P. Leffler ve Jeffrey W. Legro, *To Lead The World: American Strategy after the Bush Doctrine*, Oxford University Press, Oxford ve New York.
- FINLAN Alastair (2006). “International Security”, (ed.) Mary Buckley ve Robert Singh, *The Bush Doctrine And The War On Terrorism Global Responses, Global Consequences*, Routledge, New York.
- FLYNN Matthew J. (2008). *First Strike: Preemptive Warfare in Modern History*, Taylor & Francis, New York.
- GRAY Colin S. (Temmuz, 2007). “The Implications of Preemptive And Preventive War Doctrines: A Reconsideration”, *USA Strategic Studies Institute U.S. Army War College*, Temmuz 2007, Başlık: 17, Bölüm: 101.
- HILL Raymond R. ve MILLER John O. (2017). “A History of United States Military Simulation”, *Proceedings of the 2017 Winter Simulation Conference*, s. 198.
- IKENBERRY G. John (2002). “America’s Imperial Ambition”, *Foreign Affairs*, 81:5, 44-60.
- KARADAG Ulaş (2016). “Birleşmiş Milletler Antlaşması’na Göre Meşru Müdafaa Hakkı”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 7:2, 171-186.
- KAUFMAN Robert Gordon (2007). *In Defense of the Bush Doctrine*, The University Press of Kentucky, Kentucky.
- KEGLEY Charles W. ve RAYMOND Gregory A. (2003). “Preventive War and Permissive Normative Order.” *International Studies Perspectives*, 4:4, 385-394.
- KIRSCHENBAUM, J. (2010). “Operation Opera: An Ambiguous Success.” *Journal of Strategic Security*, 3:4, 49-62.
- KISSINGER Henry (2002). “Preemption and the End of Westphalia”, *New Perspectives Quarterly*, 19:4, 31-36.
- LAFEVER Walter (Güz 2002). “The Bush Doctrine”, *Diplomatic History*, 26:4, 543-558.
- LAYNE Christopher (2006). “The Unipolar Illusion Revisited: The Coming End of the United States’ Unipolar Moment.” *International Security*, 31:2, 7-41.

- MUELLER Karl P. CASTILLO Jasen J. MORGAN Forrest E. PEGAHI Negeen ROSEN Brian (2006). *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*, RAND Corporation, Santa Monica.
- NATIONAL RESEARCH COUNCIL (1995). *The Changing Nature of Telecommunications/Information Infrastructure*, The National Academies Press, Washington.
- PARKER, Thomas (2016). “When Churchill Bombed France.” *The National Interest*, 145, 77-84.
- PAZARCI Hüseyin (2015). *Uluslararası Hukuk*, Turhan Kitabevi, Ankara.
- REITER Dan (2005). “Preventive Attacks Against Nuclear Programs and the ‘Success’ at Osiraq”, *Nonproliferation Review*, 12:2, 355-371.
- RENSHON Stanley A. (2010). *National Security in the Obama Administration Reassessing the Bush Doctrine*, Routledge, New York.
- SCHMIDT Brian C. ve WILLIAMS Michael C. (2008). “The Bush Doctrine and the Iraq War: Neoconservatives Versus Realists”, *Security Studies*, 17, 191-220.
- THE USA NATIONAL SECURITY COUNCIL (Ekim 2002) the National Security Strategy Chapter III. Strengthen Alliances to Defeat Global Terrorism and Work to Prevent Attacks Against Us and Our Friends.
- UNITED NATIONS SECURITY COUNCIL (1981). Decision of 19 June 1981 (2288th meeting): Resolution 487.
- UNITED NATIONS SECURITY COUNCIL OFFICIAL RECORDS (15 Haziran 1981). Attack on Iraq - SecCo Debate -Verbatim record, 2282nd Meeting, New York.
- LOBEL Jules (2000). “Benign Hegemony? Kosovo and Article 2(4) of the U. N. Charter,” *Chicago Journal of International Law*, 1:1, 19-36.
- YAO Kai ve HUANG Shaoluo (2021). “Simulation Technology and Analysis of Military Simulation Training”, *Journal of Physics: Conference Series*, 1746, s. 2
- İnternet Kaynakları**
- AMAZON (2023). “Monte Carlo Simülasyonu nedir?”, <https://aws.amazon.com/tr/what-is/monte-carlo-simulation/>, erişim 11.05.2023.
- HAVELSAN (2020) “Havelsan Yapay Zekâlı Simülâtör Geliştirecek”, <https://www.havelsan.com.tr/haberler/guncel/havelsan-yapay-zekali-simulator-gelistirecek>, erişim 11.05.2023.
- INSTITUTE FOR SECURITY & DEVELOPMENT POLICY (Haziran 2018). “Made in China 2025 Backgrounder”, <https://isd.eu/content/uploads/2018/04/Made-in-China-Backgrounder.pdf>, erişim 11.05.2023.
- KOYUNCU Hüseyin (2021). “Askeri Simülasyon Basına Sızdı: Rus Ordusu Varşova’yı 4 Günde Kuşatabilir”, <https://tr.euronews.com/2021/02/06/rus-ordusu-polonya-ya-sald-r-rsa-baskent-varsova-sadece-dort-gunde-kusat-l-r>, erişim 11.05.2023.
- LACEY James (22 Nisan 2019). “How Does The Next Great Power Conflict Play Out? Lessons From A Wargame”, *War on the Rock*, <https://warontherocks.com/2019/04/how-does-the-next-great-power-conflict-play-out-lessons-from-a-wargame/>, erişim 11.05.2023.
- LINDEN LAB (2023). “About Linden Lab”, <https://www.lindenlab.com/>, erişim 11.05.2023.
- MICROSOFT (2013). “Surface Hub 2S”, <https://www.microsoft.com/en-us/surface/business/surface-hub-2>, erişim 11.05.2023.
- MICROSOFT (2015). “Diplomacy Everywhere: Microsoft donates cutting-edge technology to bring diplomacy to life for visitors of the U.S. Diplomacy Center”, <https://blogs.microsoft.com/on-the-issues/2015/02/25/diplomacy-everywhere-microsoft-donates-cutting-edge-technology-to-bring-diplomacy-to-life-for-visitors-of-the-u-s-diplomacy-center/>, erişim 11.05.2023.

- MICROSOFT (2023). “Makine öğretiminde ve pekiştirici öğrenmede konu uzmanlığını kullanma”, <https://learn.microsoft.com/tr-tr/azure/architecture/solution-ideas/articles/machine-teaching>, erişim 11.05.2023.
- MINISTRY OF FOREIGN AFFAIRS OF DENMARK (2023). “The TechPlomacy Approach”, <https://techamb.um.dk/the-techplomacy-approach>, erişim 11.05.2023.
- PRINCETON UNIVERSITY (2023). “Plan A”, <https://sgs.princeton.edu/the-lab/plan-a>, erişim 11.05.2023.
- PRINCETON UNIVERSITY (2023). “Simulating Nuclear War”, <https://sgs.princeton.edu/the-lab/simulating-nuclear-war>, erişim 11.05.2023.
- REUTERS (2007). “Sweden first to open embassy in Second Life”, <https://www.reuters.com/article/us-sweden-secondlife-idUSL3034889320070530>, erişim 11.05.2023.
- SECONDLIFE (2023). <https://secondlife.com/>, erişim 11.05.2023.
- THE NATIONAL MUSEUM OF AMERICAN DIPLOMACY (2023). “Diplomacy Simulations: Immerse students in the world of American Diplomacy”, <https://diplomacy.state.gov/education/diplomacy-simulations/>, erişim 11.05.2023.
- STEINBERG, J.B. O’HANLON, M.E., SUSAN E.R. (2002). “The New National Security Strategy and Preemption”, <https://www.brookings.edu/articles/the-new-national-security-strategy-and-preemption/>, erişim 29.06.2023.
- THE UNITED STATES MILITARY ACADEMY (2023). “West Point Simulation Center”, <https://www.westpoint.edu/military/department-of-military-instruction/simulation-center>, erişim 11.05.2023.
- THE USA NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (2020). “The Cyber Range: A Guide: Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training”, <https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420%201315.pdf>, erişim 11.05.2023.
- THE USA NATIONAL SECURITY COUNCIL (Ekim 2002). “The National Security Strategy Chapter V. Prevent Our Enemies from Threatening Us, Our Allies, and Our Friends with Weapons of Mass Destruction” <https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/nss5.html>, erişim 11.05.2023.
- THE USA THE DEPARTMENT OF DEFENSE (2023). “National Cyber Range”, <https://www.peostri.army.mil/national-cyber-range-ncr>, erişim 11.05.2023
- THE USA Virtual Embassy Iran, <https://ir.usembassy.gov/>, erişim 29.06.2023.