

Bilgi Ortamında Harekât: Bilgiye Yönelik ve Bilişsel Harp Üzerine Kavramsal Çerçeve Önerisi

Information Environment Operations: A Conceptual Framework Proposal on Knowledge-Focused Warfare and Cognitive Warfare

Osman Gazi
KANDEMİR*

* Dr. Tuğg. (E), Milli Savunma
Üniversitesi, Kara Harp Enstitüsü
Misafir Öğretim Üyesi, İstanbul,
Türkiye.
e-posta: ogkandemir@gmail.com
ORCID: 0000-0002-6283-6861

Öz

Bu çalışma, bilgi ortamında yürütülen harekâtın kavramsal çerçevesini yeniden yapılandırmayı ve Türkçe literatürdeki terminolojik karmaşayı gidermeyi amaçlamaktadır. Çalışmanın amacı iki yönlüdür: İlk olarak, literatürdeki hâkim adlandırma olan “bilgi harbi” teriminin epistemolojik ve operasyonel yetersizliklerini ortaya koyarak yerine daha kapsayıcı bir kavram önermek; ikinci olarak, bilgi ortamındaki faaliyetleri sistematik biçimde sınıflandırmaktır. Çalışma, “information warfare” teriminin Türkçeye “bilgi harbi” olarak çevrilmesinin anlam kaymasına neden olduğunu vurgulayarak, NATO doktrinleriyle uyumlu “Bilgi Ortamında Harekât” kavramını çatı terim olarak önermektedir. Bu ortam, fiziksel, sanal ve bilişsel boyutlarıyla bütünlük biçimde ele alınmaktadır. Çalışmanın temel katkısı, bilgi ortamındaki harekâtları iki ana kategoriye ayırmasıdır: Bilgiye Yönelik Harp (BYH) ve Bilişsel Harp (BH). BYH, siber ve elektronik harp gibi teknik araçlarla düşmanın bilgi sistemlerini hedeflerken; BH, etki harbi, dezenformasyon ve psikolojik operasyonlarla doğrudan insan zihnini hedefler. Modern hibrit çatışmalarda bu iki alan giderek iç içe geçmektedir. Sonuç olarak, çalışma Türk Silahlı Kuvvetleri ve ulusal güvenlik kurumları için bilgi ortamında açık ve tutarlı bir kavramsal çerçeve geliştirmenin stratejik zorunluluğunu ortaya koymakta; güvenlik çalışmaları ve stratejik iletişim alanlarında uygulayıcılara ve akademisyenlere rehberlik sağlamayı hedeflemektedir.

Anahtar Kelimeler: Bilgi Ortamında Harekât, Bilgiye Yönelik Harp, Bilişsel Harp, Etki Harbi, Stratejik İletişim

Abstract

This study aims to reconstruct the conceptual framework for operations conducted within the information environment while addressing terminological confusion in Turkish literature. It has two primary objectives: first, to expose the epistemological and operational shortcomings of the term “bilgi harbi” (information warfare) and to propose a more comprehensive alternative; second, to systematically categorize activities within the information environment. The study highlights that the Turkish translation of “information warfare” as “bilgi harbi” leads to semantic and doctrinal distortions, advocating for “Information Environment Operations” as a more fitting umbrella term compatible with NATO doctrines. This environment is examined holistically, encompassing its physical, virtual, and cognitive dimensions. The primary contribution of this study is the systematic classification of operations in the information environment into two main categories: Knowledge-Focused Warfare (KFW) and Cognitive Warfare (CW). KFW targets the enemy’s information systems using technical tools such as cyber and electronic warfare, while CW directly influences the human mind through techniques like influence warfare, disinformation, and psychological operations. In the context of modern hybrid conflicts, these two areas get increasingly intertwined. In conclusion, the study underscores the strategic necessity of developing a clear and consistent conceptual framework for information environment operations tailored to the Turkish Armed Forces and national security institutions. It also provides essential conceptual guidance for both practitioners and academics in the fields of security studies and strategic communication.

Keywords: Information Environment Operations, Knowledge-Focused Warfare, Cognitive Warfare, Influence Warfare, Strategic Communication

Geliş Tarihi / Submitted:
25.02.2025

Kabul Tarihi / Accepted:
10.11.2025

Extended Summary

This study critically examines the terminological and conceptual problems arising from the long-standing use of the term “*bilgi harbi*” (information warfare) in Turkish literature and proposes a doctrinally coherent and epistemologically consistent framework for operations in the information environment. The study’s fundamental argument is that the translation of “information warfare” into Turkish as “*bilgi harbi*” is based on both epistemological and operational flaws.

In Turkish, the concept “*bilgi*” refers to a final mental product that has been interpreted and internalized, while the English term “information” corresponds to organized data or a transmission process. This fundamental difference has made the concept of “*bilgi harbi*” inadequate for reflecting the true scope of the field. To overcome this problem, the study proposes “Information Environment Operations” as an umbrella term, which is also compatible with North Atlantic Treaty Organization (NATO) doctrines. This approach enables us to address the information environment holistically, encompassing its physical, virtual, and cognitive dimensions.

The study’s second major contribution is its division of activities conducted in the information environment into two main categories based on the ultimate nature of their objectives: Knowledge-Focused Warfare (KFW) and Cognitive Warfare (CW). This distinction is explained through the “envelope and letter” metaphor: KFW targets the envelope and postal process of the letter, while CW targets how its content is read and interpreted.

KFW is a system-oriented approach that targets the enemy’s capacity to collect, process, and transmit information. It is conducted through technical tools such as cyber warfare, electronic warfare, reflexive control, and command-and-control warfare. Its primary objective is to paralyze the adversary’s decision-making capability and establish information dominance. KFW’s strategic objectives include establishing information access superiority, directing information flow, influencing decision-making processes, protecting information sources, and maintaining information monopoly. Tools such as cyber network operations, electronic warfare, directed energy weapons, and space systems are used to achieve these objectives.

On the other hand, CW is a form of struggle that directly targets the human mind, perceptions, attitudes, and behaviors. Unlike traditional psychological warfare, this field represents a sophisticated approach that utilizes modern neuroscience and cognitive sciences, aiming to manipulate how individuals think and consequently how they behave. CW is conducted through two fundamental methods: overt activities (influence operations) and covert activities.

The Influence Warfare dimension seeks to shape the perceptions of societies, cultures, and public opinion through visible tools such as strategic communication, public diplomacy, cultural diplomacy, soft power, and digital diplomacy. Perception management, narrative construction, and reinterpretation of history are fundamental elements of this strategy. Covert activities include more complex methods such as disinformation, social engineering, reflexive control, truth decay, post-truth strategies, and neurotechnological interventions.

The study also emphasizes the interaction between KFW and CW. These two areas increasingly intertwine in the modern conflict environment, introducing a new dimension known as “hybrid information operations.” A cyberattack can not only disable technical infrastructure but also create lasting effects at the cognitive level by generating distrust and

panic in society. Russia's annexation of Crimea in 2014 and invasion of Ukraine in 2022 are examples of this hybrid approach. These cases demonstrate how technical disruptions in communication networks were synchronized with large-scale cognitive influence campaigns.

The study concludes that the center of gravity of modern warfare has shifted from the physical realm to the information and consciousness domains. Clausewitz's principle of "forcing the enemy to accept our will" is now being realized in the 21st century through algorithms, narratives, and perceptions. In this context, there emerges a strategic necessity for the Turkish Armed Forces and national security institutions to develop a clear, consistent, and hierarchical conceptual framework for operations conducted in the information environment. The terminological distinction and systematic structure proposed by the study have the potential to constitute a solid foundation for future doctrinal studies, training programs, and strategic planning.

Giriş

Savaş, tarih boyunca yalnızca fiziksel çatışmalarla değil, zihin, algı ve irade üzerinde yürütülen mücadelelerle de tanımlanmıştır. "Clausewitz'in *"Savaş, politik bir amaca ulaşmak için düşmanı irademizi kabul etmeye zorlayan bir şiddet eylemidir"*¹ tanımı, savaşın özünde iradeler arasındaki mücadele olduğunu gösterir. Sun Tzu'nun *"Kendini ve düşmanını tanıyorsan, yüz savaşın sonucundan korkmazsın"*² sözü ise bilgi üstünlüğünün zaferdeki belirleyici rolünü vurgular.

Savaşın değişmeyen doğası, onu fiziksel, bilgi ve insan boyutlarında süreklilik arz eden bir mücadeleye dönüştürmüştür. Bu boyutlar arasında köprü görevi gören bilgi boyutu, muhasımın bilgi dünyasını hedef alan propaganda, hile, aldatma ve manipülasyon gibi tekniklerle daima stratejik bir alan olmuştur. 20. yüzyılda sanayi ve teknolojiadaki gelişmeler, savaşın kapsamını genişletmiş ve yıkıcılığını artırmıştır.³ Artık savaş, sadece orduların değil, toplumların, ekonomilerin ve kültürlerin de hedef alındığı çok katmanlı bir mücadeleye evrilmiştir.

Modern savaşların en belirgin özelliklerinden biri, savaş ve barış arasındaki sınırların giderek bulanıklaşmasıdır.⁴ Devletler, klasik savaş alanlarında verdikleri mücadele kadar, toplumların zihinlerine ve algılarına yönelik stratejilere de ağırlık vermektedir. Bu durum, Miller'in "sıcak barış-sıcak savaş"⁵ tayfi yaklaşımını destekler nitelikte olup, üstünlük mücadelesinin uzaydan dijital dünyaya kadar genişleyen yeni bir harp sahasında sürdüğünü göstermektedir. Bilginin konvansiyonel mecralardan dijital platformlara aktarılması, toplumları birey bazında hedef alan asimetrik stratejilerin önünü açmıştır. Artık bilgisayarlar ve dijital sistemler kontrolünde olmayan bilgi istisna haline gelmiş, karar mekanizmaları da dijital sistemler üzerindeki eylemlere karşı hassas duruma gelmiştir.

Devletler, muharebe sahasına ihtiyaç duymadan bilgi ortamını kullanarak düşmanı zayıflatma, tarafsızları kendi yanına çekme ve kamuoylarını stratejik hedeflerine uygun şekilde yönlendirme çabasıdadır. Günümüzde savaşlar yalnızca ordular arasında değil; sosyal medya platformlarında, ekonomik pazarlarda, diplomatik masalarda ve en önemlisi toplumların zihinlerinde verilmektedir. Üçüncü küreselleşme ve dijital teknolojilerin

1 Carl von Clausewitz, *On War* (çev. Michael Howard ve Peter Paret), Princeton University Press, Princeton, 1984, s. 83.

2 Sun Tzu, *The Art of War* (çev. Samuel B. Griffith), Oxford University Press, Oxford, 1963, s. 84.

3 Christopher Bellamy, *The Evolution of Modern Land Warfare Theory and Practice*, Routledge, New York, 1984, s. 62.

4 Valery Gerasimov, "The Value of Science in Prediction", *Military-Industrial Kurier*, February 27, 2013, s. 2.

5 Benjamin Miller, *States, Nations, and the Great Powers: The Sources of Regional War and Peace*, Cambridge University Press, Cambridge, 2007, s. 47-50.

gelişmesiyle birlikte, bilgi ortamında yürütülen savaşlar daha sofistike hale gelmiş, sınırlar kalkmış ve bilginin nüfuz gücü hiç olmadığı kadar artmıştır. Siber uzaydaki dezenformasyon kampanyaları, sosyal medya manipülasyonları ve yapay zekâ destekli bilgi savaşları, modern etki harbinin temel unsurları haline gelmiştir.⁶

Bilgi ortamında yürütülen harekâtların, yeni küreselleşme ve teknolojiadaki gelişmeler sebebiyle kendine yeni alanlar bulması, güvenlik ve savaş çalışmaları alanında literatürün zenginleşmesine vesile olmuştur. Ateş ve Evren’in söylediği gibi, savaşın doğası değişmemiştir, bugün yeni gibi adlandırılan birçok mücadele biçimi tarihin ilk dönemlerinden beri vardır ama savaşın kapsadığı alan ve aktörleri değişmiştir.⁷ Bu durumda yeni kavramların ortaya çıkması bir gerekliliktir.⁸ Bu bağlamda bilgi ortamında yürütülen harekâtları tanımlamak için de çok sayıda savaş çeşidi kavramı (bilişsel, etki, psikolojik, siber, elektronik, anlatı harbi vb.) üretilmiştir. Ancak, üretilen bu kavramların sınırlarının belirlenmesi, bir alan hiyerarşisi içinde bulunmaları da bir gerekliliktir.

Bu çalışma, ilk olarak Türkçe literatüre girmiş bulunan “bilgi harbi” kavramını eleştirel biçimde incelemeyi ve bu kavramın daha isabetli bir çerçeveye yeniden tanımlanmasını amaçlamaktadır. “*Information warfare*” ifadesinin Türkçeye “bilgi harbi” olarak çevrilmesi, alanın kapsamı ve içeriği açısından çeşitli kavramsal sorunlar yaratmıştır. Bu çeviri zamanla, kavramın, insan beynini hedef alan birçok harp çeşidini içine alan şemsiye bir kavrama dönüşmesine yol açmıştır. Ancak bu kullanım hem teorik olarak muğlaktır hem de pratikte ayırıştırıcı analizlere engel teşkil etmektedir. Bu nedenle çalışmada bilgi harbi kavramı daha dar ve yerinde bir bağlama oturtulmaya çalışılacak, mevcut geniş kullanımı yerine daha kapsayıcı ve açıklayıcı bir üst kavram önerilecektir.

Çalışmanın ikinci amacı, hâlihazırda “bilgi harbi” başlığı altında birlikte anılan çok sayıda yöntem, araç ve stratejiyi daha sistematik bir yaklaşımla yeniden tasnif etmektir. Bu çerçevede bilgi ortamındaki harekâtlar, iki temel alana ayrılarak incelenecektir. Birincisi doğrudan “bilgi”nin korunması veya yok edilmesiyle ilgili harekâtlar, ikincisi ise insan beynini hedef alan harekâtlardır. Her bir alan; stratejik hedefleri, operasyonel araçları ve yöntemsel yaklaşımları bakımından ayırıştırılarak incelenecek, böylece bu alandaki kavramsal karmaşaya karşı bütüncül ama ayırt edici bir analiz çerçevesi ortaya konacaktır. Bu yaklaşım, yalnızca teorik açıklık sağlamakla kalmayacak; aynı zamanda uygulayıcılar, karar vericiler ve araştırmacılar için sağlam bir başvuru zemini oluşturacaktır.

Günümüzde savaşın boyutları yalnızca kara, deniz, hava veya siber alanlarla sınırlı değildir; bilgi, zihin ve irade üzerindeki mücadeleler de modern çatışmaların belirleyici unsuru haline gelmiştir. Bu bağlamda “bilgi boyutu”, savaşın yalnızca fiziksel varlıkları değil, aynı zamanda algı, irade ve karar süreçlerini hedef alan zihinsel uzamını ifade eder. Bu makale, savaşın bilgi boyutunun tarihsel sürekliliğini inceleyerek, bilgiye ve insana yönelik harekât biçimlerinin kuramsal temelini ortaya koymayı amaçlamaktadır.

1. Aldatmadan Günümüze Kavramların Tarihsel Evrimi

Savaşlar, tarih boyunca sadece fiziksel çatışmalarla sınırlı kalmamış, aynı zamanda zihinlerde ve psikolojik alanda da mücadelelerle şekillenmiştir. Sun Tzu’nun dediği gibi,

6 P.W. Singer ve Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, 2018, s. 88-90.

7 Barış Ateş ve Evren Mercan, “Yeni Savaşlar ve Yeni Ordular”, *Güvenlik Stratejileri Dergisi*, Özel Sayı, 2023, 1-11.

8 Çalışmanın başlangıcında yapılan literatür taramasında 102 farklı çeşit harp kavramına (ekine *warfare* kelimesi almış) rastlanmıştır.

“*Her savaş aldatmaca üzerine kuruludur.*”⁹ Düşmanın karar alma süreçlerini bozmak, yanlış yönlendirmek ve moralini bozmak için farklı taktikler kullanılmıştır. Antik çağda ordular, güçlerini abartılı göstermek için sahte mevziler kurmuş, gece boyunca ateşler yakmış ve casuslarla yanlış bilgiler yaymıştır. 14. yüzyılda Moğollar, Ceneviz kalesine vebalı cesetler fırlatarak korkuyu bir silah olarak kullanmıştır. Bu eylem, düşmanın korku ve kaos algısını hedeflemiş, bilgi üstünlüğü sağlanmıştır. Bu yöntemler, erken dönem bilgi harbi stratejileri olarak görülebilir.

Tarihsel süreçte bilgi ortamında yürütülen faaliyetleri adlandırmak için çeşitli kavramlar ve teoriler kullanılmıştır. Propaganda, bilgi harbi literatüründeki en eski kavramlardan biridir. Latince *propagare* (yaymak, çoğaltmak) kelimesinden gelir. İnsanlar, antik çağlardan beri bilinçli manipülasyon teknikleri ile birbirlerini etkilemeye çalışmıştır. Pratkanis ve Aronson’a göre propaganda, düşünce biçimlerini yönlendirmek için kullanılan sistematik bir yöntemdir ve tarih boyunca politik, ekonomik ve toplumsal alanlarda güçlü bir araç olmuştur.¹⁰

Modern anlamda propaganda, 1622’de Papa XV. Gregory’nin Katolik inancını yaymak için kurduğu *Sacra Congregatio de Propaganda Fide* (İnancın Yayılması için Kutsal Cemaat) ile sistematik hale gelmiştir.¹¹ Başlangıçta dini amaçlı kullanılan bu terim, zamanla siyasi ve ideolojik mücadelelerde de yer almıştır. Fransız Devrimi sırasında broşürler, afişler ve sloganlar, halkı etkilemek için yoğun şekilde kullanılmış, matbaanın yaygınlaşması ve okuryazarlığın artmasıyla propaganda, geniş kitlelere ulaşma imkânı bulmuştur.

20. yüzyılda bilgi ortamında harekâtın önemi artmıştır. 1928’de Edward Bernays, *Propaganda* kitabıyla modern propaganda ve kamuoyu manipülasyonunun temellerini atmış,¹² demokratik toplumlarda bile kitleleri kontrol etmek için propaganda kullanılabileceğini savunmuştur. George F. Kennan’ın politik savaş teorisi, modern bilgi harbi uygulamalarının erken ve sistematik örneklerinden biridir.¹³ Kennan, Soğuk Savaş döneminde ABD’nin Sovyetler Birliği’ne karşı uygulaması gereken stratejileri belirlemiştir. Politik harp, düşmanın siyasi, ekonomik, psikolojik ve toplumsal yapısını hedef alıyordu. ABD, bu stratejiyle Sovyetler Birliği’ne karşı propaganda, gizli operasyonlar ve psikolojik harp yöntemleri kullanmıştır. *Radio Free Europe* ve *Voice of America* gibi medya araçlarıyla Sovyet halklarına ulaşmaya çalışmıştır.

1960’ta Schelling, *The Strategy of Conflict* kitabında¹⁴ bilgi ve iletişimin çatışma stratejilerindeki rolünü incelemiş, blöf, tehdit ve güven inşası gibi kavramlara odaklanmıştır. 1964’te McLuhan, *Understanding Media*¹⁵ eserinde, medyanın algıyı nasıl şekillendirdiğini ve bunun bilgi harbinde nasıl kullanılabileceğini anlatmıştır. 1967’de Vladimir Lefebvre, “Refleksif Kontrol” kavramını geliştirmiştir. Bu strateji, düşmanın karar alma süreçlerini manipüle ederek, onu istenen yönde hareket etmeye zorlamak amacındadır.¹⁶

9 Tzu, *The Art of War*, s. 66.

10 Anthony Pratkanis ve Elliot Aronson, *Age of Propaganda: The Everyday Use and Abuse of Persuasion*, W. H. Freeman, New York, 2001, s. 37-39

11 The Catholic Encyclopedia, s.v. “Congregation for the Propagation of the Faith,” <https://www.newadvent.org/cathen/12456a.htm>, erişim 20.02.2025.

12 Edward Bernays, *Propaganda*, Horace Liveright, New York, 1928, s. 45.

13 George F. Kennan, *The Inauguration of Organized Political Warfare*, Memorandum, Policy Planning Staff, ABD Dışişleri Bakanlığı, 4 Mayıs 1948.

14 Thomas Schelling, *The Strategy of Conflict*, Harvard University Press, Cambridge, MA, 1960, s. 112.

15 Marshall McLuhan, *Understanding Media: The Extensions of Man*, McGraw-Hill, New York, 1964, s. 78.

16 Maria W. de Goeij, “Reflexive Control: Influencing Strategic Behavior,” *Parameters* 53, no. 4 (2023) s. 97-108.

1980’lerde Sovyet KGB’si ve Doğu Alman Stasi’si, dezenformasyon ve psikolojik harp operasyonlarıyla düşman ülkelerin iç siyasetini ve halkın moralini bozmuş, *Operation Infection* (AIDS’in ABD tarafından geliştirildiği yalanı) gibi kampanyalar düzenlemiştir.¹⁷ Joseph Nye, 1990’da askerî veya ekonomik güç kullanmadan kültür, değerler ve politikalarla etkilemeyi tanımlayan “yumuşak güç” kavramını ortaya atmıştır. 1994’te Albay Richard Szafranski, “*Neocortical Warfare*” (neokortikal harp) kavramını tanıtmıştır.¹⁸ Bu strateji, düşmanın karar alma süreçlerini ve algılarını manipüle ederek savaşı insan beynine taşımayı hedeflemektedir.

1999’da Çinli Albaylar Qiao Liang ve Wang Xiangsui, “Sınırsız Savaş” teorisi ile geleneksel savaşın ötesine geçip ekonomik, siyasi, teknolojik, medya ve siber alanlarda düşmanı zayıflatmayı önermişler.¹⁹ 2003’te Çin Halk Kurtuluş Ordusu, “Üç Savaş” stratejisini geliştirmiştir.²⁰ Psikolojik harp, medya harp ve hukuk harp unsurlarını içeren bu strateji, bilgi ortamını hem iç hem de dış politikada etkili şekilde kullanmayı amaçlamaktadır.

21. yüzyılda dijitalleşme ve internetin yaygınlaşmasıyla bilgi harbi yeni bir boyut kazanmıştır. Philip Taylor, modern savaşların sadece cephelerde değil, zihinlerde de kazanıldığını söylemiştir.²¹ Bilgi harbi, artık sadece devletler arasında değil, toplumların algısını şekillendirme ve yönlendirme süreçlerinde de kullanılıyordu. Hibrit harple birlikte bilgi ortamında harekâtlar yoğunlaşmıştır. Devletler hem kendilerini koruma hem de gri alanda rakiplerine karşı operasyon yapma reflekslerini geliştirmişlerdir. Günümüzde ise savaşlar, fiziksel alanların ötesine geçip beyinlere ulaşmaktadır. Dr. James Giordano’nun çalışmaları,²² beynin yeni bir harp alanı haline geldiğini göstermektedir. Bu konu, bilişsel harp başlığı altında detaylandırılacaktır.

2. Terminolojik Karmaşadan Bütüncül ve Hiyerarşik Bir Yaklaşım

Bir eylemin “savaş” olarak tanımlanabilmesi için uluslararası hukuk ve askerî bilimler disiplinlerinin bakış açısından dört temel belirleyici özellik şart koşulmuştur: Savaş, 1) öncelikle kuvvet kullanma hâlidir; 2) düşmanca bir tutum ve/veya eylem içermelidir; 3) geleneksel hukuka göre üçüncü tarafları ilgilendiren hak ve yükümlülükler de dâhil olmak üzere hukuki bir durum yaratır ve son olarak 4) savaşın faili devlettir. Bu şartlar ışığında savaş; “Devletler veya devlet grupları tarafından, millî güç unsurlarının tamamının veya bir kısmının kullanılması suretiyle icra edilen ve taraflarca savaş niteliği kabul edilen, kuvvet kullanılmasını içeren, düşmanca niyet ve/veya eylem” olarak tanımlanmak mümkündür.²³

Bu tanım, klasik savaş paradigmalarını açıklamak için yeterlidir; ancak bilgi ortamında gerçekleşen siber saldırılar, psikolojik harekâtlar, anlatı operasyonları veya bilişsel müdahaleler gibi faaliyetler, silahlı çatışma eşiğine ulaşmadıkları ve doğrudan kuvvet kullanımı içermedikleri için bu tanıma dâhil edilemezler. Bu faaliyetler, savaş sayılmak için

17 Douglas Selva ve Christopher Nehring, “Operation “Denver”: KGB and Stasi Disinformation regarding AIDS” <https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids>, erişim 20.02.2025

18 Richard Szafranski, “*Neocortical Warfare? The Acme of Skill*”, *Military Review*, 74:11, 1994, s. 41-55.

19 Qiao Liang ve Wang Xiangsui, *Unrestricted Warfare: China’s Master Plan to Destroy America*, PLA Literature and Arts Publishing House, Beijing, 1999.

20 Peter Mattis, “China’s ‘Three Warfares’ in Perspective”, *War on the Rocks*, 30 Ocak 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>, erişim 15.03.2025.

21 Philip M. Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, Manchester University Press, Manchester, 2003, s. 13, 217.

22 MWI Video: The Brain is the Battlefield of the Future – Dr. James Giordano <https://mwi.westpoint.edu/mwi-video-brain-battlefield-future-dr-james-giordano/>, erişim 10.03.2025.

23 Ali Bilgin Varlık, “Savaşı Tanımlamak: Terminolojik Bir Yaklaşım”, *Avrasya Terim Dergisi*, 1:2, 2013, s. 114-129.

gereken hukuki ve askerî eşikleri karşılamamaktadır. Bu nedenle savaş hukuku da bu alanları kapsam dışında bırakmaktadır.

Bununla birlikte, 1959 basımlı Kara Harp Okulu *Harb Tarihi*²⁴ kitabında dikkat çekici bir açılım sunulmuş; klasik savaş anlamı içinde kuvvet kullanılarak yapılan eylemler “askerî harp” ya da “silahlı harp” olarak özel başlık altına alınmış, buna karşılık diğer mücadele biçimleri de savaş çerçevesinde değerlendirilmiştir. Bu yaklaşım, savaş kavramının yalnızca fiziki kuvvete indirgenmemesi gerektiğine işaret etmesi bakımından önemlidir.

Bu çerçevede, bilgi ortamında yürütülen çok sayıda faaliyet, klasik anlamda “savaş” sayılmasa da Clausewitz’in iradeyi zorlama amacını modern teknoloji ve bilişsel bilimler aracılığıyla gerçekleştirme çabalarıdır. Bu eylemler, sistemli, örgütlü ve düşmanca niyetle yürütüldükleri ve stratejik hedeflere ulaşmak için millî gücün tüm unsurlarını (bilgi, psikoloji, teknoloji) kullandıkları için “harp” olarak adlandırılabilirler.²⁵

Alanın Türkçe literatür açısından bir başka problemi “war” (savaş) ve “warfare” (savaşma biçimi) kavramlarının Türkçede ayrı ayrı karşılığının bulunmamasıdır. Bu konunun incelenmesi makalenin konusu dışındadır. Ancak bütünlük ve anlaşılabilirlik açısından kolaylık olsun diye “war” karşılığında “savaş”, “warfare” karşılığında “harp” kelimeleri kullanılmıştır.

2.1. Bilgi Harbi Kavramının Yeterliliği ve Çatı Kavram Önerisi

Çalışmanın ana konusu olan “Bilgi harbi” kavramı Türkçe literatüre, İngilizce “information warfare” kavramı üzerinden girmiştir. Türkçedeki “bilgi” kelimesi, eski Türkçeden bu yana kullanılan “bil-” fiilinden türetilmiştir. Bu fiil “kavramak”, “öğrenmek”, “farkında olmak” anlamları taşır. Fiil köküne eklenen “-gi” yapım ekiyle türetilen “bilgi”, doğrudan doğruya “bilinen şey” yani zihinde anlamlandırılmış, içselleştirilmiş içerik anlamına gelir.²⁶ Bu yönüyle Türkçedeki “bilgi” kavramı, insan zihninde oluşmuş ve anlam kazanmış nihai bir bilişsel ürünü ifade eder.

Buna karşılık, İngilizcedeki “information” kelimesi Latince *informare* fiilinden türemiştir. Bu fiil, “biçim vermek”, “şekillendirmek” anlamlarına gelir; *informatio* ise bir zihni dışsal veriler aracılığıyla şekillendirme sürecini ifade eder.²⁷ Modern anlamda “information”, genellikle verinin anlamlı biçimde düzenlenmiş hali, yani bir iletişim veya aktarım süreci olarak tanımlanır. Ancak bu içerik, bireyin zihninde anlam kazanıp özümsemedikçe “bilgi” (*knowledge*) haline gelmiş sayılmaz.²⁸

Türk Dil Kurumu, “information” terimini “danışma” ve “haberleşme” olarak karşılamakta; Ötügen Sözlük²⁹ ve Kubbealtı Lugatı³⁰ da benzer biçimde “bilgilendirme, haber verme, veri iletme” gibi anlamlar vermektedir. Bunun yanı sıra “information” kelimesinin Türkçeye, malumat³¹ olarak çevrildiği de vakidir. Dolayısıyla “information warfare” teriminin “bilgi harbi” olarak çevrilmesi, Türkçedeki “bilgi” kavramının derinliği göz önünde bulundurulduğunda, çeviri düzeyinde önemli bir kaymaya yol açmaktadır.

24 Orhan Ergüder, *Harb Tarihi*, Kara Harp Okulu Basımevi, Ankara, 1959; akt.; Varlık a.g.m.

25 Paul A. Smith, Jr., *On Political War*, National Defense University Press, Washington D.C. 1989, s. 3.

26 Gerard Clauson, *An Etymological Dictionary of Pre-Thirteenth-Century Turkish*, Clarendon Press, Oxford, 1972, s. 330.

27 “Information”, *Online Etymology Dictionary*, <https://www.etymonline.com/word/information>, erişim 15.10.2025.

28 Luciano Floridi, *The Philosophy of Information*, Oxford University Press, Oxford, 2011, s. 93-107.

29 Yaşar Çağbayır, *Orhun Yazıtlarından Günümüze Türkiye Türkçesinin Söz Varlığı Ötügen Türkçe Sözlük*, İstanbul, Ötügen Yayınları, 2007, s. 1448.

30 İlhan Ayverdi, *Misallı Büyük Türkçe Sözlük*, Kubbealtı Yayınları, İstanbul, 2010, s. 344.

31 Türkçe’deki enformasyon harbine bilgi harbi denmesinin yarattığı bulanıklığı gidermek için Dağhan Yet, “malumat harbi” kavramını önermiştir. Dağhan Yet, “Malumat Savaşında Hızlı-Etki Yaklaşımı: Türkiye Deneyimi”, Barış Ateş (ed.), *Türkiye’de Askerî Yenilik*, Vakıfbank Kültür Yayınları, İstanbul, 2023, s. 315-341.

İngilizcedeki *information* kelimesinin karşılığı olarak Türkçeleşmiş bir kelime olan “enformasyon”, ham verinin düzenlenmesi ve anlam kazanmasını sağlayan soyut bir yapıya sahiptir, ancak tek başına bilgi değildir. Bilgi, ancak enformasyonun işlenmesi, anlamlandırılması ve bireyler veya sistemler tarafından yorumlanmasıyla ortaya çıkar.³² Bu bağlamda, enformasyon, bilgiye giden yolda kritik bir ara aşamadır ve onu kontrol eden aktörler, bilgi üretme ve karar alma süreçlerinde üstünlük sağlayabilirler. İletişim Başkanlığı tarafından yayınlanan sözlükte de “Bilgi Harbi” kavramı bulunmazken “Enformasyon Savaşları” kavramına yer verilmiştir.³³

Türk Silahlı Kuvvetlerine ait askerî terimler sözlüklerinde “bilgi harbi” terimi bulunmamaktadır. Yayınlanmış taktik ya da doktriner belgelerde de bu kavrama rastlanmaz. Ancak Dışişleri Bakanlığının çevrim içi “Askerî Terimler Sözlüğü”nde “*information warfare*” terimi doğrudan “bilgi harbi” olarak çevrilmiştir. Bu çeviri eğilimi, çevrim içi sözlüklerde de yaygındır. Ancak bu uygulama, kavramın yalnızca sözcük düzeyinde karşılığını vermekte; içerik ve kapsam bakımından önemli belirsizlikleri beraberinde getirmektedir.

ABD ordusunun yeni uygulamaya başladığı “Çok Alanlı Muharebe Doktrininde” harekâtın icra edildiği çevre (*operational environment*), üç temel boyutta ele alınmaktadır: fiziksel çevre, insan boyutu ve enformasyon boyutu. Bu modelde temel unsur “bilgi” (*knowledge*) değil, “enformasyon” (*information*) olarak tanımlanır.³⁴ Çünkü askerî harekât ortamında aktarılan, yönlendirilen ve hedeflenen içerik, genellikle anlam kazanmamış ham veri ya da düzenlenmiş enformasyondur. Karar destek sistemleri, komuta-kontrol yapıları ve bilişsel etki süreçlerinin çoğu, henüz bireysel anlamlandırma süzgecinden geçmemiş bu enformasyon türü üzerine inşa edilir.

Bilgi kuramlarında bu ayırım daha da netleştirilmiştir:

- Veri (*data*), işlenmemiş ham ölçümlerdir.
- Enformasyon (*information*), düzenlenmiş ve bağlama yerleştirilmiş veridir.
- Bilgi (*knowledge*) ise enformasyonun anlamlandırılarak zihinde kavranmış, içselleştirilmiş hâlidir.³⁵

Bu ayırım doğrultusunda her bilgi, zamanında bir enformasyondur; ancak her enformasyon, bilgiye dönüşmeyebilir. Dolayısıyla “*information warfare*” teriminin “bilgi harbi” şeklinde çevrilmesi, bilgi ile enformasyonun hem epistemolojik hem de operasyonel düzeyde farklı şeyler olduğu gerçeğini göz ardı etmektedir.

Yukarıda ifade edilen anlam kaymasına ilave olarak, “bilgi harbi” terimi çoğu zaman çatı kavram gibi kullanılmakta; siber harp, bilişsel harp, psikolojik harp, etki operasyonları ve anlatı harbi gibi çok sayıda kavram bu başlık altında toplanmaktadır. Ancak yukarıda açıklanan nedenlerle “bilgi harbi” kavramı hem epistemolojik açıdan hem de terminolojik bakımdan bu alanı kuşatmak için yetersizdir.

Bu çalışma, bu noktada bilgiye yönelik faaliyetlerin bütününe içerecek şekilde “Bilgi Ortamında Harekât” (*Information Environment Operations*) kavramını kavramsal çatı olarak önermektedir. Bu yaklaşım, enformasyonun üretimi, dağıtımı, yönlendirilmesi ve kontrolü yoluyla yürütülen tüm operasyonları birleştiren daha kapsayıcı bir çerçeve sunar.

32 Malik Yılmaz, “Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi”, *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi* 49, no. 1 (2009): 95-118.

33 İletişim Başkanlığı, *Stratejik İletişim Terimleri Sözlüğü*, Ankara, 2025, s. 56.

34 FM 3-0: *Operations*, Headquarters, Department of the Army, Washington, D.C., 2022, s.1-16,1-18.

35 Malik Yılmaz, a.g.m.

“Bilgi ortamı” kavramı Kuzey Atlantik Antlaşması Örgütü (*North Atlantic Treaty Organization* - NATO) doktrinlerine girmiştir. Dokümanlar, Bilgi Ortamı (BO) değerlendirmesinde BO’yu birbirleriyle etkileşim halinde olan üç temel boyutta ele almaktadır. Bu boyutlar, BO’daki eylemlerin basamaklı ve çok katmanlı etkilerini analiz etmek için temel bir çerçeve sunmaktadır:

- Fiziksel Boyut: Bilginin işlendiği ve iletildiği altyapıyı, donanımı ve insanları içerir. Komuta-kontrol merkezleri, iletişim ağları, sunucular, personel ve silah sistemleri bu boyutun temel unsurlarıdır.
- Sanal Boyut: Bilginin yaratıldığı, işlendiği ve paylaşıldığı ağlar, siber sistemler ve elektromanyetik spektrumu kapsar. Bu boyut, verinin kendisinin bulunduğu alandır.
- Bilişsel Boyut: İnsanların bilgiyi algıladığı, yorumladığı, inanç ve tutumlarını oluşturduğu ve nihayetinde karar verip davranışa dönüştürdüğü zihinsel alandır. Harekâtın nihai hedefi bu boyutta etki yaratmaktır.

Bu boyutlar sıralı değil, iç içe geçmiştir. Örneğin bir fiber optik kabloya yönelik fiziksel bir saldırı (fiziksel boyut), bağlantıyı kesintiye uğratarak (sanal boyut) hasım bir aktörün bu bilgi boşluğunu dezenformasyonla doldurup hedef kitlede panik veya güvensizlik yaratmasına (bilişsel boyut) olanak tanıyabilir. Bu nedenle etkili planlama, etkilerin bu boyutlar arasında nasıl basamaklandığını anlamayı gerektirir.

Türk Silahlı Kuvvetleri’nin doktrin geliştirme yaklaşımı açısından da bu yapı önemlidir. Nitekim Türk Silahlı Kuvvetleri (TSK), “hibrit harp” yerine “hibrit ortamda harekât” terimini kullanmakta; bu tercih, çatışmanın farklı boyutlarının eşzamanlı ve bütünsel karakterine vurgu yapmaktadır. Benzer biçimde, NATO doktrinleriyle uyumlu olarak “Bilgi Ortamında Harekât” kavramının da TSK literatürüne dâhil edilmesi, bilgi ortamında yürütülen faaliyetlerin stratejik ve doktriner bütünlük içinde ele alınmasına katkı sağlayacaktır.

Ortam, bilginin basit bir veri akışından ibaret olmadığını, aksine onu yorumlayanların önyargıları, gündemleri ve kişisel yorumlama süreçleri gibi sosyal, kültürel ve psikolojik faktörlerle şekillendiğini gösterir. Konunun stratejik önemi de tam olarak bu noktada yatmaktadır: Bilgi Ortamı, en nihayetinde stratejik karar verme süreçlerinin gerçekleştiği temel ortamdır. NATO doktrini, bu karmaşık ortamı anlamlandırmak için “Bilgi Ortamı Değerlendirmesi (*Information Environment Assessment* – IEA)” olarak bilinen analitik bir süreç öngörmektedir.³⁶ Bu ortamda üstünlük kuran bir aktör, rakibinin kararlarını ve dolayısıyla eylemlerini şekillendirme yeteneği kazanır. Bilgi Ortamı’nın bu çok katmanlı yapısını anlamak, içinde yürütülen farklı harekât türlerini doğru sınıflandırmanın ve stratejik hedeflere uygun araçları seçmenin temelini oluşturur.

2.2. Bilgi Ortamında Harekâtın İki Ana Boyutu

Bu çalışmanın ikinci adımı, bilgi ortamında yürütülen harekâtları, hedefin nihai doğasına göre iki temel kategoriye ayırmaktır. Bu ayırım, harekâtın “bilginin kendisine veya iletimini sağlayan teknik sistemleri mi”, yoksa “bilginin yorumlandığı insan bilişimini mi” hedef aldığına dayanmaktadır. Bu sınıflandırma, kullanılan araçlar ile ulaşılmak istenen stratejik etki arasındaki farkı netleştirmektedir.

³⁶ NATO, *Allied Joint Doctrine for Information Operations (AJP-10)*, NATO, Brussels, 2021, s. 40.

2.1.1. Bilgiye Yönelik Harp (Knowledge-Focused Warfare):

Bu kategori, doğrudan bilgi sistemlerinin, veri zincirlerinin ve karar destek altyapılarının hedef alındığı faaliyetleri içerir. Amaç, karşı tarafın bilgi edinmesini engellemek, bilgi süreçlerini bozmak ya da bilgi üretimini yönlendirmektir. Bu alanın içerisine Siber harp, elektronik harp, bilgi güvenliği operasyonları, veri akışını manipüle etme, bilgi tekeline koruma gibi hususlar girer.

Bu tür operasyonlar genellikle teknik ve sistem düzeyinde yürütülür. Hedef, insan bilinci değil; veri akışları, komuta-kontrol sistemleri ve askerî karar döngüleridir.

2.1.2. Bilişsel Harp (Cognitive Warfare):

Bilgi ortamındaki ikinci ana faaliyet alanı, doğrudan insan zihnini, algılarını, tutumlarını ve davranışlarını hedef alan harekâtlardır. Bu tür operasyonlarda fiziksel değil bilişsel etki hedeflenir. Bilgiye yönelik harp, bilginin kendisine ve akışına odaklanırken, Bilişsel Harp bilginin ötesine geçerek beynin o bilgiyle ne yapacağını hedefler. Bu nedenle bu mücadele, “bilginin kendisi üzerine değil, bilginin anlamı üzerine bir savaştır”.

2.1.3. Zarf ve Mektup Metaforu: Bilgi Akışı mı, Biliş mi?

BYH ile BH arasındaki farkı açıklamak için “zarf ve mektup” metaforu öğretici bir çerçeve sunmaktadır. Bu metafora, iletişim süreci bir mektubun gönderilmesi ve okunması üzerinden düşünülmüştür.

BYH, mektubun zarfını ve posta sürecini hedef alır. Yani mesajın alıcıya doğru, zamanında ve bütünlük içinde ulaşmasını sağlayan sistemlere müdahale eder. Amaç, bilgi akışını engellemek, zayıflatmak veya bozarak iletişim zincirini kırmaktır. Siber harekât bu alanın en somut örneğidir; mesajın fiziksel veya sanal taşıyıcılarını —ağları, sunucuları, kabloları— hedef alır. Bu, “mektubun yolda kaybolması, gecikmesi veya zarfının hasar görmesi” durumuna benzetilebilir.

Bilişsel Harp (BH) ise mektubun kendisine, yani içeriğin nasıl okunduğu ve anlamlandırıldığına odaklanır. Mektup alıcıya ulaşmıştır; fakat amaç, alıcının onu gönderenin istediği biçimde yorumlamasını sağlamaktır. Burada hedef bilgi akışı değil, bilginin anlamıdır. Bilişsel harp, insanların ne düşündüğünü değil, nasıl düşündüğünü ve davrandığını şekillendirmeyi hedefler. Bu nedenle bilişsel düzeyde yürütülen operasyonlar, mesajın gerçekliğini değil, algısını dönüştürmeyi amaçlar. Bu metafor, bilgi ortamında yürütülen harekâtların iki temel yönünü sade biçimde ayırır:

BYH bilginin taşınma sürecini, BH ise bilginin anlamlandırılma sürecini hedef alır.

Modern savaş ortamında bu iki süreç çoğu zaman iç içe geçer; bir zarfın yırtılması, mektubun içeriğine dair güvensizlik yaratabileceği gibi, yanlış yazılmış bir mektup da göndericinin güvenilirliğini zedeleyebilir. Dolayısıyla bilgi akışına yönelik teknik müdahaleler ile bilişsel algıyı hedefleyen psikolojik operasyonlar, çağdaş çatışmalarda birbirini tamamlayan araçlar hâline gelmiştir.

Çalışmanın bundan sonraki bölümlerinde Bilgi Ortamında Harp’in alt kolları analiz edilecektir.

3. Bilgiye Yönelik Harp: Modern Çatışmada Sistem-Odaklı Strateji

Modern savaşta çatışmanın ağırlık merkezi, fiziksel alanlardan bilgi alanına kaymaktadır. “Bilgiye Yönelik Harp” (BYH), hasmın karar verme döngülerini, komuta-kontrol mekanizmalarını ve bilgi altyapısını doğrudan hedef alan sistem odaklı bir stratejik

yaklaşımdır. Geleneksel psikolojik harbin aksine, insan bilincini değil, bilginin kendisini işleyen sistemleri merkezine alır.³⁷

3.1. BYH'nin Temel Nitelikleri

Hedef: Bilgi sistemleri, veri zincirleri ve komuta-kontrol altyapılarıdır. Düşmanın bilgisayar ağlarından sensörlerine, iletişim uydularından radar sistemlerine kadar geniş bir yelpazedeki teknik varlıkları hedefler.

Amaç: Karşı tarafın bilgi edinmesini engellemek, bilgi süreçlerini bozmak ve bilgi üretimini yönlendirmek. Temel gaye, düşmanın durumsal farkındalığını ortadan kaldırmaktır.

Odak Noktası: İnsan bilinci yerine veri akışları, sensörler, ağlar ve askerî karar döngüleri (OODA döngüsü). BYH, bir komutanın moralini bozmak yerine, o komutanın emir almasını sağlayan iletişim ağını çökertmeye odaklanır.³⁸

3.2. Stratejik Hedefler

Bilgiye Erişim Üstünlüğü: Bilgi üstünlüğü, bir tarafın kendi bilgi faaliyetlerini serbestçe yürütürken, hasmının aynı faaliyetleri yürütmesini engelleme yeteneğidir.³⁹ Nihai amaç, “karar üstünlüğü” elde etmektir. Karar üstünlüğü, bir komutanın rakibinden daha etkili kararlar alarak operasyonel inisiyatifi ele geçirmesi anlamına gelir.⁴⁰

Bilgi Akışını Yönlendirmek: Bu hedef, düşmanı aktif olarak yanlış yönlendirmeyi amaçlar. Rus askerî düşüncesindeki “Refleksif Kontrol” teorisi, düşmana sahte dayanaklar sunarak onu kendi iradesiyle bizim istediğimiz yönde kararlar almaya itmeyi hedefler.⁴¹ Düşmanın sensör ağlarını karıştırma gibi eylemler, karar vericinin önüne yanlış bir operasyonel resim koyar.⁴²

Karar Alma Süreçlerini Etkilemek: BYH, OODA döngüsünün özellikle “Gözlemle” ve “Yönel” aşamalarına müdahale eder. Amaç, düşmanın karar kalitesini düşürmek ya da karar verme süresini kritik eşiğin üzerine çıkarmaktır.⁴³

Bilgi Kaynaklarını Korumak: Dost bilgi altyapısını düşmanın faaliyetlerinden korumak, en az saldırmak kadar önemlidir. Bu hedef, Operasyon Güvenliği (OPSEC) ile doğrudan ilişkilidir ve BYH'nin defansif ayağının temelini oluşturur.⁴⁴

Bilgi Tekelini Elde Bulundurmak: Çatışma bölgesindeki bilgi akışını kontrol etmek, bir gücün kendi anlatısını hem askerî hem de sivil alanda tek geçerli referans noktası haline getirmesini sağlar. Çin'in “Üç Savaş” doktrininin bir parçası olan “kamuoyu savaşı”, tam olarak bu hedefe hizmet eder.⁴⁵

37 John Arquilla ve David Ronfeldt, “The Advent of Netwar: Analytic Background”, *Studies in Conflict & Terrorism* 22:3, 1999, s. 193-206.

38 Edward Waltz, *Information Warfare Principles and Operations*, Artech House, Boston, 1998, s. 16.

39 Martin C. Libicki, “What is Information Warfare?” *ACIS Paper 3*, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, Washington, DC, 1995, s. 94.

40 Headquarters, Department of the Army, *FM 3.0, Operations*, Washington, D.C.: Department of the Army, 2022, s. 3-72.

41 Timothy L. Thomas, “Russia's Reflexive Control Theory and the Military”, *Journal of Slavic Military Studies* 17:2, 2004, s. 237-256.

42 Libicki, “What is Information Warfare?”, s. 29.

43 North Atlantic Treaty Organization, *Comprehensive Operations Planning Directive COPD V3.1*, NATO, Brussels, 2023, s. 4-71.

44 NATO, *AJP-10*, s. 2-19.

45 Peter Mattis, “China's ‘Three Warfares’ in Perspective”.

3.3. Temel Araçlar ve Yöntemler

Siber Ağ Harekâtları: Siber savaş, BYH'nin en bilinen aracıdır ve düşmanın bilgisayar sistemlerini hedef alır.⁴⁶ NATO doktrininde siber uzay, kara, deniz ve hava gibi ayrı bir harekât alanı olarak tanımlanmıştır.⁴⁷ Siber saldırıların faili tespit etmek zordur. Fransız TV5 Monde'a yapılan ve başlangıçta IŞİD tarafından üstlenilen saldırı, daha sonra Rusya bağlantılı APT28 hacker grubunun "sahte bayrak" operasyonu olduğu ortaya çıkmıştır.⁴⁸

Elektronik Harp: Elektromanyetik spektrumu kullanarak düşman radar, iletişim ve seyrüsefer sistemlerini hedef alır. Uygulamaları arasında düşman sinyallerini bastırarak (*jamming*) veya sahte hedefler yaratarak (*deception*) durumsal farkındalığını yok etmek bulunur.⁴⁹

Yönlendirilmiş Enerji Silahları: Elektromanyetik darbe (EMP) kullanarak elektronik devreleri fiziksel olarak tahrip edebilirler. Rus askerî yazarları, Batı'nın ağ merkezli savaş üstünlüğüne karşı asimetrik bir yanıt olarak bu silahların potansiyelini sıkça dile getirmektedir.⁵⁰

Uzay Sistemleri: Modern orduların komuta-kontrol, iletişim ve istihbarat yetenekleri büyük ölçüde uydulara bağımlıdır.⁵¹ Düşman uydularını hedef almak, bir ülkenin tüm askerî ve sivil iletişim altyapısını felç etme potansiyeline sahiptir.⁵²

3.4. Değerlendirme

FM 3-0 doktrini, siber alanı eylemin gerçekleştirildiği mekân; bilgi boyutunu ise etkinin odaklandığı alan olarak tanımlar. BYH bu köprüyü operasyonel düzeye indirger: siber, elektromanyetik ve uzay araçlarıyla karar üstünlüğü elde etmeyi hedefler.⁵³

BYH, karşı tarafın fizikî gücü yerine bir devletin sinir sistemi —bilgi işleme ve karar verme yeteneğini— hedef alır. Geleneksel psikolojik harbin odağı insan zihni iken BYH odağını makineler ve komuta-kontrol sistemlerine çevirir. Yapay zekâ, kuantum bilişim ve otonom sistemlerin yaygınlaşması BYH'yi daha merkezi bir alana taşımaktadır; bu yüzden doktrin geliştirmek ve teknolojik yetenek kazanmak artık ulusal güvenliğin temel gerekliliğidir.⁵⁴

4. Bilişsel Harp (Cognitive Warfare)

Bilişsel Harp, bilgi ortamındaki harekâtın ikinci ana boyutunu oluşturur. Fiziksel bir etki yerine bilişsel bir etki yaratmayı amaçlayan, insan zihnini, algılarını, tutumlarını ve davranışlarını hedef alan bir mücadele biçimidir.⁵⁵ Bu yaklaşım, "bilginin kendisi üzerine değil, bilginin

46 Varlık, Savaşı Tanımlamak: Terminolojik Bir Yaklaşım".

47 NATO, *COPD V3.1*, a.g.e., s.3-39.

48 Pascal Brangetto, Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations" ed.Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* Tallinn: NATO CCDCOE Publications, Talinn, 2015, 98.

49 David Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House, Boston, 2001, s. 3.

50 Age, s. 4.

51 Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies*, 27:1, 2014, 101-130.

52 Yaakov Katz ve Amir Bohbot, *The Weapon Wizards*, St. Martin's Press, New York, 2017.

53 *FM 3.0, Operations*, s.1-17/1-23.

54 Dean S. Hartley III ve Kenneth O. Jobson, *Cognitive Superiority: Information to Power*, Springer International, Cham, 2021, s. 25-133.

55 NATO, *Cognitive Warfare*, NATO, Brussels, 2023, 1-3.

anlamı üzerine bir savaştır.”⁵⁶ Nihai hedef, hedef kitlenin düşünce yapısını ve ardından eylemlerini etkilemektir. Başka bir deyişle, BH, bir hedef kitlenin nasıl düşündüğünü ve dolayısıyla nasıl davrandığını manipüle etme sanatıdır.⁵⁷

Bu yaklaşım, bilgi ortamındaki diğer operasyonlardan temel bir farkla ayrılır. Bilgiye yönelik geleneksel operasyonlar teknik sistemlere odaklanırken, BH doğrudan insanın karar alma süreçlerini hedef alır.

4.1. Stratejik Hedefler ve Değişen Paradigma

Geleneksel askerî ve hükümet yapıları hedef olmaya devam etse de birincil savaş alanı artık rakip veya tarafsız bir ulusun kamu bilincini de kapsayacak şekilde genişlemiştir. Bu paradigma değişimi, çatışmayı sürekli hale getirmekte ve barış ile savaş arasındaki çizgileri bulanıklaştırmaktadır.

Bir ulusun kamuoyunu etkilemek artık belirleyici bir faktör olarak görülmektedir. Hükümetlerin başarısı, Edward Bernays’ın belirttiği gibi, “rıza gösteren bir kamuoyuna” bağlıdır.⁵⁸ Bir aktör, kamu algısını şekillendirerek bir hükümetin meşruiyetini sarsabilir, ulusal iradeyi aşındırabilir ve geleneksel askerî eylemlerden çok daha düşük maliyetlerle stratejik hedeflerine ulaşabilir. Bu yaklaşım, ABD Stratejik Hizmetler Ofisi’nin (OSS) 1943 tarihli dokümanında belirtilen “askerî eylem dışındaki yollarla irademizi düşmana dayatmak” hedefiyle uyumludur.⁵⁹ Bu, hasmın karar alma süreçlerini felç etmek ve toplumsal uyumu bozmak suretiyle, fiziksel bir çatışmaya gerek kalmadan zafer elde etmek anlamına gelir.

4.2. Bilişsel Harp Yöntemleri

BH yöntemleri, bilişsel çevreyi şekillendirmek üzere tasarlanmış, açık ve ikna edici angajmandan gizli ve manipülatif eylemlere kadar geniş bir yelpazede faaliyet gösterir.

4.2.1. Açık faaliyetler:

Bilişsel harbin açık biçimleri genellikle etki operasyonları olarak tanımlanır. Bu faaliyetler, toplumların, kültürlerin ve karar vericilerin algılarını yönlendirmeye yönelik, doğrudan görünür stratejilerdir. Etki harbi; stratejik iletişim, kamu diplomasisi, kültürel diplomasi, yumuşak güç ve dijital diplomasi gibi araçlarla yürütülür. Yöntemlerinden bazıları aşağıda sunulmuştur.

Algı Yönetimi, devlet, lider veya olay hakkındaki algının sistematik biçimde şekillendirilmesini ifade eder. Medya manipülasyonu, kamuoyu araştırmaları, devlet destekli ajanslar ve propaganda mekanizmalarıyla desteklenir.⁶⁰ Özellikle kriz dönemlerinde algı yönetimi, rakip aktörlerin itibarsızlaştırılması ve kendi eylemlerinin meşrulaştırılması amacıyla yoğun biçimde kullanılır.

Stratejik İletişim, müttefikleri kazanmak, tarafsızları yönlendirmek ve düşmanları caydırmak için bütünlük söylemler üretmeyi amaçlar. Lider konuşmaları, semboller ve medya içerikleri üzerinden ulusal irade yaratılır.⁶¹

56 Steve A. Tatham, *Strategic Communication: A Primer*, Defence Academy of the United Kingdom, Shrivenham, 2008, s. 2.

57 Oliver Backes ve Andrew Swab, “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States”, Harvard Kennedy School, Belfer Center for Science and International Affairs, November 2019. <https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states>, erişim: 15 Ekim 2025

58 Edward Bernays, *Propaganda*, H. Liveright, New York, 1928, s.10.

59 Jr., *On Political War*, s. 226.

60 Walter Lippmann, *Public Opinion*, Harcourt, Brace and Company, New York, 1922, s. 33-35.

61 Richard Halloran, “Strategic Communication”, *Parameters*, 38:3, 2007.

Kamu Diplomasisi, doğrudan halklar arasındaki iletişim üzerinden etki kurmayı hedefler. Edmund Gullion'un 1965'te kavramsallaştırdığı kamu diplomasisi, devletlerin güvenlik ve çıkarlarını korumak için yürüttükleri iletişim faaliyetlerini içerir.⁶² Günümüzde yumuşak gücün önemli bir unsuruna dönüşmüştür.⁶³

Kültürel Diplomasi, ulusal çıkarların kültürel anlatılar yoluyla desteklenmesidir. Güney Kore'nin K-Pop ve K-Drama endüstrileri veya Çin'in Konfüçyüs Enstitüleri, başarılı örnekler arasındadır.

Yumuşak Güç Araçları (insani yardım, eğitim, barış gücü programları), zorlayıcı olmayan yollarla etki yaratır. ABD'nin Peace Corps programı veya Türkiye'nin Afrika'daki insani yardım faaliyetleri bu kapsamda değerlendirilebilir.

Dijital Diplomasi, liderlerin ve hükümetlerin sosyal medya üzerinden yürüttüğü diplomatik etki faaliyetlerini kapsar.⁶⁴ Donald Trump'ın dış politika mesajlarını Twitter aracılığıyla doğrudan vermesi veya Zelenskiy'nin küresel kamuoyuna video mesajlarıyla seslenmesi çarpıcı örneklerdir.

Etki harbi yalnızca söylem düzeyinde yürütülmez; aynı zamanda bilgi ve coğrafya üzerinden de şekillenir. *Tarihin Yeniden Yazımı*, ulusal kimlikleri ve kolektif hafızayı değiştirme amacı taşır.⁶⁵ *Jeo-uzamsal Manipülasyon*, haritalar, uydu görüntüleri ve coğrafi verilerin politik amaçlarla çarpıtılmasıdır.⁶⁶

Etki harbinin son aşaması küresel kamuoyu yönetimidir. Bu düzeyde, devletler politikalarını meşrulaştırmak için uluslararası medya, BM kararları ve hukuk söylemlerini seferber eder.⁶⁷ Rusya'nın Ukrayna'daki eylemlerini "savunma hakkı" çerçevesinde sunması, Batı'nın ise "insan hakları" vurgusuyla karşı anlatı geliştirmesi, bu stratejinin iki yönünü oluşturur.⁶⁸

4.2.2. Örtülü faaliyetler:

Bilişsel harbin örtülü biçimleri, bireylerin bilinç düzeyini hedef alır ve manipülasyonu doğrudan zihin düzeyinde gerçekleştirir. Bu kapsamda dezenformasyon, sosyal mühendislik, refleksif kontrol, gerçekliğin çürütmesi, gerçek sonrası stratejileri ve nöroteknolojik müdahaleler öne çıkar.

Bilgi Manipülasyonu, doğru bilginin çarpıtılması veya yanlış bilgiyle yer değiştirmesi yoluyla hedefin algısının yönlendirilmesidir. Yanlış bilgi (*misinformation*) bilinçsizce; dezenformasyon (*disinformation*) ise kasıtlı biçimde yayılır. Malenformasyon ise doğru bilginin bağlamından kopararak zarar verme amacıyla kullanılmasıdır.

62 İletişim Başkanlığı, *Stratejik İletişim ve Stratejik Yönetim*, İletişim Başkanlığı Yayınları, Ankara, 2023, s. 26.

63 Abdullah Özkan, 21. *Yüzyılın Stratejik Vizyonu: Kamu Diplomasisi ve Türkiye'nin Kamu Diplomasisi İmkânları*, TASAM Kamu Diplomasisi Enstitüsü, 2021, s. 18.

64 İletişim Başkanlığı, *Stratejik İletişim ve Stratejik Yönetim*, s. 99-101.

65 Margaret MacMillan, *Dangerous Games: The Uses and Abuses of History*, Modern Library, New York, 2009, s. 14-15.

66 Bakınız: Dr. Michael Izady, "Infographs, Maps and Statistics Collection", <https://gulf2000.columbia.edu/maps.shtml>, erişim: 15 Ekim 2025; Avusturya İç İşleri Bakanlığı, "Ortadoğu ve Kuzey Afrika Atlası", https://www.ecoi.net/en/file/local/1408000/90_1487770786_2017-02-bfa-mena-atlas.pdf, erişim: 15 Ekim 2025; "Cartorient", <https://cartorient.cnrs.fr/accueil>, erişim: 15 Ekim 2025; Michael Izady'nin haritaları, Kürt nüfusunu olduğundan fazla gösterdiği için Kürdologlar tarafından bile eleştirilmiştir. Kürdolog ve İranolog Garnik Asatryan, Kürdoloji'deki sözde-tarihcilik hakkında bilgi verirken İzedi'nin "1992 tarihli Kürtler: Bir El Kitabı"ndan "fantazmagorik" olarak bahseder. Garnik Asatryan, "Prolegomena to the Study of the Kurds," *Iran and the Caucasus*, 13:1, 2009, s. 1-57.

67 Philip M. Taylor, "Public Diplomacy and Strategic Communications," *The Hague Journal of Diplomacy*, 3:3, 2008, s. 1-11.

68 Lawrence Freedman, *Ukraine and the Art of Strategy*, Oxford University Press, Oxford, 2019, s. 99-102.

Psikolojik Operasyonlar, düşmanın moralini bozmak ve davranışlarını yönlendirmek için propaganda tekniklerinden yararlanır.⁶⁹ Günümüzde sosyal medya trol ağları, sahte video içerikleri ve yapay etiket (*hashtag*) kampanyaları bu süreci dijital boyuta taşımıştır. İkinci Karabağ savaşında Azerbaycan'ın drone görüntülerini kısa videolarla göstermesi etkili bir psikolojik operasyon örneğidir.

Sosyal Mühendislik, bireyleri manipüle ederek bilgi sızdırma ve gizli verilere erişim amacı taşır. “İnsan korsanlığı” olarak da bilinen bu yöntem, *phishing* ve kimlik avı teknikleriyle uygulanır.⁷⁰

Gerçekliğin Çürümesi (Truth Decay), nesnel bilginin değerinin azaldığı, görüş ve deneyimlerin gerçeğin yerini aldığı bir süreci ifade eder.⁷¹ Deepfake videolar, sahte haber siteleri ve sosyal medya botları, gerçek ile yalan arasındaki sınırı silikleştirir.

Gerçek Sonrası (Post-Truth) stratejiler, duyguların ve kişisel inançların nesnel gerçeklerin önüne geçtiği bir ortam yaratır.⁷² 2016'daki Brexit referandumu ve ABD başkanlık seçimleri, bu stratejinin tipik örnekleridir. Sosyal medya algoritmaları, yankı odaları ve filtre balonları aracılığıyla bireyler yalnızca kendi inançlarına uygun bilgileri görür.

Kutuplaştırma, bilişsel harbin hem sonucu hem aracıdır.⁷³ Toplamları ideolojik, etnik veya dini çizgiler boyunca bölerek iç istikrarsızlık üretir.

Refleksif Kontrol, düşmanın kendi iradesiyle hatalı kararlar almasını sağlamak için geliştirilen bir Rus stratejisidir.⁷⁴ Yanıltıcı istihbarat, sahte veriler ve çarpıtılmış bilgiyle, hedefin karar döngüsü manipüle edilir.

Neokortikal Harp, karar vericilerin bilişsel süreçlerine doğrudan müdahale ederek, OODA döngüsünü kırmayı hedefler.⁷⁵ Bilgi blokajı, aşırı veri yüklemesi ve psikolojik baskı yöntemleriyle düşmanın stratejik düşünme kapasitesi zayıflatılır.

Anlatı Harbi, olayların nasıl yorumlandığını değiştirerek kolektif hafızayı dönüştürür.⁷⁶ Sinema, medya ve dijital platformlarda kurgulanan hikâyeler, toplumların geçmiş algısını yeniden şekillendirir.

Nöroteknolojik Müdahaleler, bilişsel harbin en ileri aşamasıdır. Dr. James Giordano'ya göre, beyin modern çatışmaların “yeni savaş alanıdır.”⁷⁷ Elektromanyetik dalgalar, kimyasal ajanlar veya yapay zekâ destekli psikolojik analizlerle askerî personelin moral düzeyleri etkilenebilir.

69 Psikolojik Operasyonlar (*Psychological Operations (PSYOP)*) – Geleneksel olarak kullanılan terimdir, ancak ABD Savunma Bakanlığı bu terimi *Military Information Support Operations (MISO)* olarak değiştirmiştir. Joint Chiefs of Staff, JP 3-13.2, *Military Information Support Operations (MISO)*, Joint Chiefs of Staff, Washington, DC, 2014.

70 “Sosyal Mühendislik Nedir?”, <https://www.kaspersky.com.tr/resource-center/definitions/what-is-social-engineering> erişim 20.02.2025.; M. Zekeriyâ Gündüz ve Resul Daş, “Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri”, <https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf>, erişim 20.02.2025.

71 “About Truth Decay”, RAND Corporation, <https://www.rand.org/research/projects/truth-decay/about-truth-decay.html> erişim 23.02.2025.

72 Lee McIntyre, *Post-Truth*, The MIT Press, Cambridge, MA, 2018, s. 5-7.; Matthew d’Ancona, *Post-Truth: The New War on Truth and How to Fight Back*, Ebury Press, London, 2017, s. 12-15.

73 Shanto Iyengar ve Sean J. Westwood, “Fear and Loathing Across Party Lines: New Evidence on Group Polarization”, *American Journal of Political Science*, 59:3, 2015, s. 690-707.

74 Timothy L. Thomas, “Russia’s Reflexive Control Theory”.

75 Richard Szafranski, “Neocortical Warfare”, John Arquilla ve David Ronfeldt (ed.), *Athena’s Camp: Preparing for Conflict in the Information Age*, RAND Corporation, Santa Monica, CA, 1997.

76 Ajit Maan, “Narrative Warfare”, *RealClearDefense*, https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html, erişim 21.02.2025.

77 James Giordano, “Brain as the Battlefield of the Future”, YouTube video, 1:02:30, uploaded by Modern War Institute, September 25, 2018, <https://www.youtube.com/watch?v=N02SK9yd60s>, erişim 21.02.2025.

4.3. Değerlendirme

BH, çağdaş çatışma doktrinlerinde fiziksel güç kullanımının yerini alan stratejik bir paradigma değişimini temsil eder. Açık faaliyetler, toplumların algısını ve uluslararası meşruiyeti hedeflerken, örtülü faaliyetler bireylerin bilinç süreçlerini kontrol altına alır.

Bu iki boyut birbirini tamamlar: Etki operasyonları kamuoyu düzeyinde “görünür alanı”, BH ise “zihin alanını” yönetir. Dijital çağda bu sınır tamamen silinmiş, savaşın nihai hedefi insan bilinci olmuştur.

Devletlerin, örgütlerin ve teknolojik platformların bilgi üzerindeki hakimiyeti, aynı zamanda zihin üzerindeki hakimiyet anlamına gelmektedir. Bu nedenle “bilişsel güvenlik” artık ulusal güvenliğin yeni cephesidir. Bu cephede üstünlük, tanklar veya füzelerle değil; anlatılar, algoritmalar ve algılarla sağlanmaktadır.

BH, klasik savaşın sınırlarını aşarak, insanın düşünme biçimini stratejik bir hedefe dönüştürmüştür. Bu nedenle geleceğin çatışmaları, toprak kazanmak için değil, zihinleri yönetmek için yürütülecektir.

5. Hibrit Etkileşim

Bilgiye Yönelik Harp ile Bilişsel Harp kavramsal olarak farklı hedeflere odaklanmakla birlikte, modern çatışma ortamında birbirini besleyen ve tamamlayan iki bütünleşik alan haline gelmiştir. BYH teknik sistemleri, veri zincirlerini, haberleşme ağlarını ve komuta-kontrol altyapılarını hedef alarak düşmanın bilgi üretim ve aktarım kapasitesini zayıflatırken; BH bu teknik etkinin sonuçlarını insan zihnine, algısına ve karar süreçlerine yönlendirir. Böylece bilgi ortamında yürütülen harekâtlar, hem fiziksel-dijital hem de bilişsel-psikolojik düzeyde etki üretir.

Bu iki alan arasındaki etkileşim, modern savaşlarda “hibrit bilgi harekâtı” olarak adlandırılabilir. Hibrit bilgi harekâtı, teknik müdahaleyle algısal manipülasyonun senkronize biçimde kullanılması anlamına gelir. Örneğin bir siber saldırı yalnızca bir altyapıyı devre dışı bırakmak için değil, aynı zamanda toplumda güvensizlik, panik veya moral çöküntüsü yaratmak için planlanabilir. Böylece teknik bir operasyon, bilişsel düzeyde kalıcı sonuçlar doğurur. Tersine, geniş kapsamlı dezenformasyon kampanyaları da teknik sistemleri aşırı yükleyerek veya iletişim hatlarını manipüle ederek operasyonel sonuçlar üretebilir.

NATO doktrinleri açısından bakıldığında, bu hibrit yapı “bilgi ortamının çok-alanlı entegrasyonu” (*information environment's cross-domain integration*) olarak tanımlanır. AJP-10 ve AJP-3 serisi doktrinlerde bilgi ortamı; fiziksel, sanal ve bilişsel katmanların karşılıklı bağımlılık içinde olduğu bir ekosistem olarak ele alınır. Dolayısıyla bir katmanda yaratılan etki diğerine zincirleme biçimde yansır. Bu yaklaşım, bilgi ortamındaki harekâtların artık belirli bir alana hapsedilemeyeceğini, bunun yerine çok katmanlı ve senkronize biçimde icra edilmesi gerektiğini göstermektedir.

Rusya’nın 2014 Kırım ilhakı ve 2022 Ukrayna işgali, bu hibrit etkileşimin en somut örneklerindendir. 2014’te iletişim hatlarının kesilmesi, paralel biçimde yürütülen medya operasyonları ve sahte haber kampanyalarıyla desteklenmiş; siber saldırılar, bilgiye erişimi kısıtlarken, eşzamanlı dezenformasyon, Ukrayna kamuoyunun moralini zayıflatmayı hedeflemiştir. Bu süreçte BYH ve BH faaliyetleri arasında keskin bir sınır kalmamış, bilişsel sonuç doğuran teknik eylem kalıbı kurumsallaşmıştır. Aynı stratejik yaklaşım 2022’de de yinelenmiş; dronelar, GPS bozucular ve elektronik harp sistemleriyle desteklenen bilgi saldırıları, kamuoyunun algısal yönlendirilmesiyle birleştirilmiştir.

Sonuç olarak hibrit bilgi ortamı harekâtı, savaşın hem “görünür” hem “görünmez” alanlarını eş zamanlı kullanan, teknik yıkımı algısal manipülasyonla bütünleştiren yeni bir harekât biçimidir. Bu durum, bilgi ortamında üstünlük sağlamanın yalnızca teknik kapasiteyle değil, bilişsel direnç ve toplumsal farkındalık unsurlarıyla da doğrudan ilişkili olduğunu ortaya koymaktadır.

Sonuç

Bu çalışma, bilgi ortamında yürütülen harekâtların kavramsal çerçevesini yeniden yapılandırmak ve Türkçe literatürde uzun süredir devam eden terminolojik karmaşayı gidermek amacıyla hazırlanmıştır. Çalışmanın ilk bulgusu, “bilgi harbi” teriminin hem epistemolojik hem de operasyonel açıdan yetersiz kaldığıdır. Türkçede “bilgi” kavramı, anlamlandırılmış ve içselleştirilmiş bir zihinsel ürünü ifade ederken, İngilizce “*information*” terimi düzenlenmiş veri veya aktarım sürecine karşılık gelir. Bu fark, doğrudan çeviriyle oluşturulan “bilgi harbi” kavramının hem anlam hem de kapsam bakımından hatalı bir temele oturduğunu göstermektedir.

Bu nedenle çalışma, “bilgi harbi” teriminin yerine, bilgiye, insan zihnine ve karar süreçlerine yönelik tüm faaliyetleri kapsayan daha bütüncül bir kavram olarak “Bilgi Ortamında Harekât” veya “Bilgi Ortamında Harp” terimini önermektedir. Bu kavram, NATO’nun AJP-10 ve AJP-10.1 doktrinlerinde tanımlanan “*Information Environment*” anlayışıyla uyumludur. Böylece bilgi ortamı; fiziksel, sanal ve bilişsel boyutlarıyla birlikte ele alınmış; bu üç alanın karşılıklı etkileşimi, modern savaşın temel dinamiği olarak konumlandırılmıştır.

Çalışmanın ikinci temel amacı, bilgi ortamında yürütülen faaliyetleri sistematik biçimde sınıflandırmaktır. Bu hedef, bilgi ortamındaki harekâtların nihai hedeflerine göre iki ana kategoriye ayrılmasıyla karşılanmıştır: Bilgiye Yönelik Harp ve Bilişsel Harp.

BYH, sistem-odaklıdır. Düşmanın bilgi toplama, işleme ve iletim kapasitesini hedef alır; siber harp, elektronik harp, refleksif kontrol ve komuta-kontrol savaşı gibi teknik araçlarla yürütülür. Amaç, hasmın karar verme yeteneğini felç etmek ve bilgi üstünlüğü sağlamaktır. BH ise insan zihnini, algılarını ve tutumlarını hedef alır. Etki harbi, psikolojik operasyonlar, dezenformasyon kampanyaları, anlatı inşası ve nöroteknolojik müdahaleler gibi araçlarla toplumların düşünme biçimlerini dönüştürmeyi amaçlar.

Bu iki alan arasındaki fark, hedefin mahiyetindedir: BYH bilginin kendisine, BH ise bilginin anlamına yöneliktir. Ancak günümüz hibrit çatışma ortamında bu iki alan giderek iç içe geçmekte, bir siber saldırı bilişsel bir etki üretebilmekte, bir dezenformasyon kampanyası da stratejik karar mekanizmalarını doğrudan etkileyebilmektedir. Bu durum, bilgi ortamındaki operasyonların çok katmanlı doğasını ve disiplinler arası niteliğini açıkça göstermektedir.

Modern savaşın ağırlık merkezi artık fiziksel alandan bilgi ve bilinç alanına kaymıştır. Clausewitz’in “düşmanı irademizi kabul etmeye zorlama” ilkesi, 21. yüzyılda tanklar ve tüfeklerle değil, algoritmalar, anlatılar ve algılarla gerçekleştirilmektedir. Dijitalleşme, yapay zekâ, kuantum bilişim ve nöroteknolojideki ilerlemeler, bilgi ortamında harekâtın hem kapsamını genişletmiş hem de etkisini derinleştirmiştir. Bu nedenle, savaşın geleceği artık “toprak kazanmak”tan çok, “zihinleri yönetmek”le ilgilidir.

Bu bağlamda, Türk Silahlı Kuvvetleri ve ulusal güvenlik kurumlarının bilgi ortamında yürütülen harekâtlara ilişkin açık, tutarlı ve hiyerarşik bir kavramsal çerçeve geliştirmesi stratejik bir zorunluluktur. Mevcut doktrinlerdeki kavramsal belirsizlik hem akademik düzeyde anlaşılabilirliği hem de operasyonel düzeyde etkinliği sınırlamaktadır. Bu

çerçevede, Türk Silahlı Kuvvetleri’nin “hibrit ortamda harekât” yaklaşımında olduğu gibi, “Bilgi Ortamında Harekât” kavramının da doktrin ve eğitim sistemine dâhil edilmesi, bilgi ortamında üstünlük arayışını kurumsal düzeyde güçlendirecektir. Böyle bir kavramsal uyum, Türkiye’nin hem NATO doktrinleriyle eşgüdümünü artıracak hem de bilgi boyutunda bağımsız harekât planlama kapasitesine teorik bir temel sağlayacaktır. Bu çalışmanın önerdiği terminolojik ayırım ve sistematik yapı, gelecekteki doktrin çalışmaları, eğitim programları ve stratejik planlamalar için sağlam bir temel teşkil etme potansiyeline sahiptir.

Sonuç olarak, çalışma iki temel amacına ulaşmıştır:

- Türkçe literatürde “bilgi harbi” kavramının yarattığı terminolojik ve doktriner sorunları eleştirel biçimde analiz etmiş, yerini alabilecek bütünleştirici bir üst kavram önermiştir.
- Bilgi ortamındaki faaliyetleri hedefin doğasına göre ikili bir yapıda sistemleştirerek, kavramsal hiyerarşi ve teorik açıklık sağlamıştır.

Bu çerçeve, komuta-kontrol doktrinlerinin bilgi ortamına uyarlanması, bilişsel dayanıklılık eğitimleri ve sivil-asker bilgi iş birliği modelleriyle somutlaştırılabilir.

Bilgiye hükmeden, anlamı yöneten ve bilişsel çevreyi şekillendiren aktörlerin, modern savaşın ve barışın gerçek belirleyicileri olduğu açıktır. Geleceğin çatışmaları artık fiziksel alanlarda değil, insan zihninin sınırlarında yaşanacaktır. Bilgi ortamında üstünlük kuramayan hiçbir devlet, konvansiyonel gücü ne olursa olsun, stratejik rekabette kalıcı bir üstünlük elde edemeyecektir.

Çıkar Çatışması

Bu çalışmada çıkar çatışması teşkil edebilecek durum ve/veya ilişki bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Eserler

- ADAMY David (2001). *EW 101: A First Course in Electronic Warfare*, Artech House, Boston.
- ARQUILLA John ve RONFELDT David (1999). “The Advent of Netwar: Analytic Background”, *Studies in Conflict & Terrorism*, 22:3, 193-206.
- ASATRIAN Garnik (2009). “Prolegomena to the Study of the Kurds”, *Iran and the Caucasus*, 13:1, 1-57.
- ATEŞ Barış ve MERCAN Evren (2023). “Yeni Savaşlar ve Yeni Ordular”, *Güvenlik Stratejileri Dergisi*, Özel Sayı, 1-11.
- AYVERDİ İlhan (2010). *Misalli Büyük Türkçe Sözlük*, Kubbealtı Yayınları, İstanbul.
- BELLAMY Christopher (1984). *The Evolution of Modern Land Warfare Theory and Practice*, Routledge, New York.
- BERNAYS Edward (1928). *Propaganda*, Horace Liveright, New York.
- BRANGETTO Pascal ve VEENENDAAL Matthijs A. (2015). “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations”, *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn.

- ÇAĞBAYIR Yaşar (2007). *Orhun Yazıtlarından Günümüze Türkiye Türkçesinin Söz Varlığı – Ötüken Türkçe Sözlük*, Ötüken Yayınları, İstanbul.
- CLAUSEWITZ Carl von (1984). *On War* (çev. Michael Howard ve Peter Paret), Princeton University Press, Princeton.
- CLAUSON Gerard (1972). *An Etymological Dictionary of Pre-Thirteenth-Century Turkish*, Clarendon Press, Oxford.
- D'ANCONA Matthew (2017). *Post-Truth: The New War on Truth and How to Fight Back*, Ebury Press, London.
- DE GOEIJ Maria W. (2023). “Reflexive Control: Influencing Strategic Behavior”, *Parameters*, 53:4, 97-108.
- ERGÜDER Orhan (1959). *Harb Tarihi*, Kara Harp Okulu Basımevi, Ankara.
- FLORIDI Luciano (2011). *The Philosophy of Information*, Oxford University Press, Oxford.
- FREEDMAN Lawrence (2019). *Ukraine and the Art of Strategy*, Oxford University Press, Oxford.
- HALLORAN Richard (2008). “Strategic Communication”, *Parameters*, 38:3, 4-14
- HARTLEY Dean S. III ve JOBSON Kenneth O. (2021). *Cognitive Superiority: Information to Power*, Springer International, Cham, 25-133.
- HEADQUARTERS DEPARTMENT OF THE ARMY (2022). *FM 3-0: Operations*, Washington, D.C.
- İLETİŞİM BAŞKANLIĞI (2023). *Stratejik İletişim ve Stratejik Yönetim*, İletişim Başkanlığı Yayınları, Ankara.
- İLETİŞİM BAŞKANLIĞI (2025). *Stratejik İletişim Terimleri Sözlüğü*, İletişim Başkanlığı Yayınları, Ankara.
- IYENGAR Shanto ve WESTWOOD Sean J. (2015). “Fear and Loathing Across Party Lines: New Evidence on Group Polarization”, *American Journal of Political Science*, 59:3, 690-707.
- JOINT CHIEFS OF STAFF (2014). *JP 3-13.2, Military Information Support Operations (MISO)*, Joint Chiefs of Staff, Washington, D.C.
- KATZ Yaakov ve BOHBOT Amir (2017). *The Weapon Wizards*, St. Martin's Press, New York.
- KENNAN George F. (1948). *The Inauguration of Organized Political Warfare*, Memorandum, Policy Planning Staff, ABD Dışişleri Bakanlığı, 4 Mayıs 1948.
- LIBICKI Martin C. (1995). “What is Information Warfare?”, ACIS Paper 3, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, Washington, D.C.
- LIPPMANN Walter (1922). *Public Opinion*, Harcourt, Brace and Company, New York.
- MACMILLAN Margaret (2009). *Dangerous Games: The Uses and Abuses of History*, Modern Library, New York.
- McINTYRE Lee (2018). *Post-Truth*, The MIT Press, Cambridge, MA.
- McLUHAN Marshall (1964). *Understanding Media: The Extensions of Man*, McGraw-Hill, New York.
- MILLER Benjamin (2007). *States, Nations, and the Great Powers: The Sources of Regional War and Peace*, Cambridge University Press, Cambridge.
- NATO (2021). *Allied Joint Doctrine for Information Operations (AJP-10)*, NATO, Brussels.
- NATO (2023). *Cognitive Warfare*, NATO, Brussels.
- NORTH ATLANTIC TREATY ORGANIZATION (2023). *Comprehensive Operations Planning Directive (COPD) V3.1*, NATO, Brussels.
- ÖZKAN Abdullah (2021). *21. Yüzyılın Stratejik Vizyonu: Kamu Diplomasisi ve Türkiye'nin Kamu Diplomasisi İmkânları*, TASAM Kamu Diplomasisi Enstitüsü.
- PRATKANIS Anthony ve ARONSON Elliot (2001). *Age of Propaganda: The Everyday Use and Abuse of Persuasion*, W. H. Freeman, New York.
- QIAO Liang ve WANG Xiangsui (1999). *Unrestricted Warfare: China's Master Plan to Destroy America*, PLA Literature and Arts Publishing House, Beijing.
- SCHELLING Thomas (1960). *The Strategy of Conflict*, Harvard University Press, Cambridge, MA.
- SINGER P.W. ve BROOKING Emerson T. (2018). *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston.
- SMITH Paul A. Jr. (1989). *On Political War*, National Defense University Press, Washington D.C.
- SUN Tzu (1963). *The Art of War* (çev. Samuel B. Griffith), Oxford University Press, Oxford.
- SZAFRANSKI Richard (1994). “Neocortical Warfare? The Acme of Skill”, *Military Review* 74:11, 41-55.
- SZAFRANSKI Richard (1997). “Neocortical Warfare”, *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla ve David Ronfeldt, RAND Corporation, Santa Monica, CA, Bölüm 17.
- TATHAM Steve A. (2008). *Strategic Communication: A Primer*, Defence Academy of the United Kingdom, Shrivenham.

- TAYLOR Philip M. (2003). *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, Manchester University Press, Manchester.
- TAYLOR Philip M. (2008). “Public Diplomacy and Strategic Communications”, *The Hague Journal of Diplomacy*, 3:3, 1-11.
- THOMAS Timothy (2014) Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?, *The Journal of Slavic Military Studies*, 27:1, 101-130.
- THOMAS Timothy L. (2004). “Russia’s Reflexive Control Theory and the Military”, *Journal of Slavic Military Studies*, 17:2, 237-256.
- VARLIK Ali Bilgin (2013). “Savaşı Tanımlamak: Terminolojik Bir Yaklaşım”, *Avrasya Terim Dergisi*, 1:2, 114-129.
- WALTZ Edward (1998). *Information Warfare: Principles and Operations*, Artech House, Boston.
- YET Dağhan (2023). “Malumat Savaşında Hızlı-Etki Yaklaşımı: Türkiye Deneyimi”, Barış Ateş (ed.), *Türkiye’de Askeri Yenilik*, Vakıfbank Kültür Yayınları, İstanbul, 315-341.
- YILMAZ Malik (2009). “Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi”, *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49:1, 95-118.

İnternet Kaynakları

- About Truth Decay, RAND Corporation, <https://www.rand.org/research/projects/truth-decay/about-truth-decay.html>, erişim 23.02.2025.
- AVUSTURYA İÇ İŞLERİ BAKANLIĞI, “Ortadoğu ve Kuzey Afrika Atlası”, https://www.ecoi.net/en/file/local/1408000/90_1487770786_2017-02-bfa-mena-atlas.pdf, erişim 15.10.2025.
- BACKES Oliver ve SWAB Andrew (2019). “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States”, Harvard Kennedy School, Belfer Center for Science and International Affairs, <https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states>, erişim 15.10.2025.
- Cartorient, <https://cartorient.cnrs.fr/accueil>, erişim 15.10.2025.
- GERASIMOV Valery (2013). “The Value of Science in Prediction”, Military-Industrial Kurier https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, erişim 21.02.2025.
- GIORDANO James (2018). “Brain as the Battlefield of the Future”, YouTube video, Modern War Institute, <https://www.youtube.com/watch?v=N02SK9yd60s>, erişim 21.02.2025.
- GÜNDÜZ M. Zekeriya ve DAŞ Resul, Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri, <https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf>, erişim 20.02.2025.
- Information. Online Etymology Dictionary, <https://www.etymonline.com/word/information>, erişim 15.10.2025.
- IZADY Michael, “Infographs, Maps and Statistics Collection”, <https://gulf2000.columbia.edu/maps.shtml>, erişim 15.10.2025.
- MAAN Ajit (2018). “Narrative Warfare”, RealClearDefense, https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html, erişim 21.02.2025.
- MATTIS Peter (2018). “China’s ‘Three Warfares’ in Perspective”, War on the Rocks, 30 Ocak 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>, erişim 15.03.2025.
- MWI, “MWI Video: The Brain is the Battlefield of the Future – Dr. James Giordano”, <https://mwi.westpoint.edu/mwi-video-brain-battlefield-future-dr-james-giordano/>, erişim 10.03.2025.
- SELVAGE Douglas ve NEHRING Christopher, Operation “Denver”: KGB and Stasi Disinformation regarding AIDS, <https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids>, erişim 20.02.2025.
- Sosyal Mühendislik Nedir?, <https://www.kaspersky.com.tr/resource-center/definitions/what-is-social-engineering>, erişim 20.02.2025.
- The Catholic Encyclopedia, s.v. “Congregation for the Propagation of the Faith,” <https://www.newadvent.org/cathen/12456a.htm>, erişim 20.02.2025.