SİBER GÜVENLİK TEHDİDİ OLARAK DEZENFORMASYON: DİJİTAL GÜVENLİK VE DİPLOMASİ AÇISINDAN ETKİLERİ

Hüma Gül ÇAKIR*
ORCID ID: 0000-0003-2796-1058

Declaration*

Abstract

The circulation of information has experienced significant transformations on a global scale with the development and acceleration of digitalization. While this transformation has made access to information easier, it has also created the conditions for maniplative content and disinformation to spread rapidly and on a large scale. The main question of this article is why disinformation is increasingly viewd as a cyber security threat and how it affects diplomatic processes in the contemporary digital environment. The article applied a qualitative research method based on document analysis and case study methodology. Academic literature and institutional reports were examined to investigate the transformation of disinformation and conceptualization as a cyber threat. Case study such as 2026 U.S. presidential election, the Brexit referendum and the Russian-Ukraine War were analyzed tos how the effects and political consenquences of cyber-enabled disinformation. The findings indicate that disinformation has become an integral part of the cyber space today. States and other actors in the cyber space are engage in disinformation activities by using social media platforms, algorithmic dissemination, data analysis and Al-generated content and thereby achieve various objectives. In this regard, it appears that disinformation disseminated in the cyber space can be understood as a multidimensional phenomenon at the intersection of cyber security, strategic communication and diplomacy.

Keywords: Disinformaiton, Cyber Security, Information Operations, Digital Diplomacy

Özet

Dijitalleşmenin gelişimi ve hızlanmasıyla bilgi dolaşımı küresel ölçekte önemli dönüşümler yaşamıştır. Bu dönüşüm bilgiye erişimi kolaylaştırırken aynı zamanda manipülatif içeriklerin

* Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü, Doktora öğrencisi, humagulcakir@gmail.com
* Bu çalışmanın yazım sürecinde makale organizasyonunun oluşturulması, yabancı dil çevirisi ve dilsel düzenleme amacıyla yapay zeka araçları kullanılmıştır.

ve yanlış bilgilerin de hızlı ve geniş ölçekte yayılmasına zemin hazırlamıştır. Bu makalenin temel sorusu, dezenformasyonun neden giderek artan bir siber güvenlik tehdidi olarak görüldüğü ve çağdaş dijital ortamda dezenformasyonun diplomatik süreçleri nasıl etkilediğini inceleme üzerinedir. Makalede belge analizi ve vaka incelemesi metodolojisine dayalı nitel araştırma yöntemi kullanılmıştır. Dezenformasyonun dönüşümünü ve siber tehdit olarak kavramsallaştırılmasını incelemek için akademik literatür ve kurumsal raporlar incelenmiştir. 2016 ABD Başkanlık seçimleri, Brexit referandumu, Rusya-Ukrayna Savaşı gibi seçilen örnekler ise siber destekli dezenformasyonun yansımalarını ve siyasi sonuçlarını göstermek için analiz edilmiştir. Bulgular, dezenformasyonun günümüzde siber alanın ayrılmaz bir parçası haline geldiğini göstermektedir. Devletler ve diğer siber alan aktörleri, sosyal medya platformlarının, algoritmik yayılımların, veri analizinin ve yapay zekâ üretimi içeriklerin kullanılması yoluyla dezenformasyon faaliyetleri oluşturulmakta ve bunun sonucunda çeşitli hedeflere ulaşabilmektedir. Bu bağlamda siber ortamda yayılan dezenformasyonun, siber güvenlik, stratejik iletişim ve diplomasi kesişiminde çok boyutlu bir olgu olarak anlaşılması mümkün görünmektedir.

Anahtar Kelimeler: Dezenformasyon, Siber Güvenlik, Bilgi Operasyonu, Dijital Diplomasi

Giriş

Bilgiye erişim ve bilgi kullanımı, tarihin her safhasında hem bireyler hem de devletler için büyük önem taşımıştır. Bu noktada başarılı olan aktörler hem siyasi hem de ekonomik olarak bilgi gücünün avantajlarından yararlanmışlardır. Küreselleşme ile bilgi ve iletişim teknolojilerinin artması, dünya çapındaki en önemli gelişmelerden biri olan dijitalleşmenin önünü açarak hem bireylerin hem de ulusların iletişimlerini dijital ağlar aracılığıyla gerçekleştirmelerine neden olmuştur. Bu dönüşümle birlikte bilginin ve iletişimin uluslararası sistemdeki rolü değişmiş ve yeni bir güvenlik alanı doğmuştur. Teknoloji ilerledikçe, geleneksel uluslararası güvenlik ortamının sınırları ortadan kalkmaya başlamış ve teknolojik alanın güvenliği ön plana çıkmaya başlamıştır. Bu bağlamda bilginin ve onun güvenliğinin sağlanması hem ulusal hem de uluslararası alanda uluslararası güvenliğin önemli bir bileşeni haline gelerek siber güvenlik, bilgi güvenliği ve dijital güvenlik gibi modern kavramların ortaya çıkmasına sebep olmuştur.

Nye, uluslararası politikada bilgi ve güç arasındaki ilişkiyi analiz ederken bilginin çeşitli boyutlarının analiz edilmesi gerektiğini belirtmektedir. Bu noktada birinci olarak bilgi,

haberler, istatistikler ve kamuya açık bilgi biçimleri de dahil olarak sınırlar arası veri akışını ifade edebilir. Son yıllarda bu sınır ötesi bilgi akışları genişlerken, bilgiye erişim ve iletim maliyetleri düşmüş ve dijital teknolojiler sayesinde erişim noktaları sayısı artmıştır. Bu dönüşüm sayesinde daha küçük devletler ve devlet dışı aktörler küresel bilgi ağına daha aktif katılım sağlamışlardır. İkinci olarak bilgi, stratejik veya ekonomik rekabette avantaj elde etmek için kullanılan bir kaynak olarak kullanılabilir. Bu noktada bilginin zamanlaması önemlidir çünkü rakiplerden daha önce bilgi edinen ve kullanan aktörler avantaj elde ederler. Rekabetçi bilgiler genelde ekonomik faaliyetler ile ilişkilendirilse de askeri alanlarda da bilgi üstünlüğünün sonuçları önemlidir. Üçüncü olarak bilgi, potansiyel rakiplerin niyetleri, kapasiteleri ve planları hakkında stratejik bilgi olarak belirlenmektedir. Stratejik bilgiler, uluslararası arenanın merkezinde olan istihbarat ve casusluk gibi uygulamalarla ilişkilendirilebilir. Teknolojik gelişmeler belirli istihbarat araçlarını genişleterek daha fazla aktörün bilgi toplamasına olanak sağlasa da avantajlı konum hala büyük ve daha geniş kaynaklara sahip olan devletlerin elindedir (Nye, 2002, s. 68).

Bilgi mücadeleleri, devletlerin hem barış hem de kriz dönemlerinde siyasi hedeflerine ulaşmak için kullandıkları önemli bir araç haline gelmiştir. Uluslararası ilişkiler rekabet ve iş birliğinin eş zamanlı var olduğu bir yapıya sahip olduğu için bilgi üzerindeki mücadeleler uluslararası sistemin kalıcı bir özelliği olarak görülmektedir. Bilgi üretimi, yayılımı ve kamuoyu algısını şekillendirme faaliyetleri bilgi etkisindedir. Bu çerçevede dezenformasyonun yayılması, bilgi akışlarının manipülasyonu gibi uygulamalar önemli etki araçlarını oluşturmaktadır (Talinshinsky, 2026, s. 7). Günümüzde sosyal medya, algoritmik manipülasyon, bot ağları, deepfake teknolojileri gibi yeni faaliyetler dezenformasyonu çok daha etkili ve ölçeklenebilir hale getirmiştir. Bu nedenle dezenformasyon artık sadece bir propaganda aracı değil, siber güvenlik tehdidi (Caramancion, 2020), hibrit savaş aracı (Bērziņš, 2014) veya diplomatik ilişkileri etkileyen bir stratejik araç (Nye, 2019) olarak görülebilir.

Çalışmanın temel sorusu siber güvenlik, uluslararası ilişkilerde ve diplomatik süreçlerde dezenformasyonla mücadeleye nasıl bir katkı sağlar şeklinde oluşturulmuştur. Alt sorular olarak dezenformasyonun neden siber güvenlik tehdidi olarak görüldüğü, dezenformasyonla mücadele için hangi siber güvenlik stratejilerinin kullanılması gerektiği ve bu stratejilerin uluslararası diplomasi ve normları nasıl etkilediği şeklinde belirlenmiştir. Bu bağlamda

makalede uluslararası ilişkilerde bilginin stratejik kullanımına odaklanarak dezenformasyon, siber güvenlik ve diplomasi arasındaki ilişkiye değinilmiştir.

Dezenformasyon ve Siber Güvenlik

Dezenformasyon Kavramı

Dijital iletişim teknolojilerinin artan önemi, çağdaş toplumlarda bilgi üretimi, dolaşımı ve tüketimini temelden dönüştürdüğü görülmektedir. Bilgi kavramı giderek artan şekilde dijital platformlar ve ağ tabanlı iletişim sistemleri üzerinden akmaya devam ederken içeriklerin hızlı yayılması hem ulusal hem de uluslararası siyasi ortamlarda yeni fırsatlar yaratırken yeni güvenlik açıkları da yaratmaktadır. İletişim teknolojileri, sosyal medya platformları ve siber alandaki gelişmeler hem devletlerin hem de devlet dışı aktörlerin bilgiyi daha önce görülmemiş bir ölçekte yayma kapasitelerini genişletmiştir. Bu noktada küreselleşme ile dijital teknolojilerin artan öneminin, uluslararası arenada aktörlerin bilgiyi siyasi süreçleri ve kamuoyunu etkilemek için kullanabilecekleri bir kaynağa dönüştürdüklerini söylenebiliriz. Bilgi uluslararası ilişkilerde önemli bir etki aracı haline gelirken dezenformasyon faaliyetleri yoluyla bilginin manipülasyonu hem siber güvenlik hem de diplomasi için giderek daha önemli bir zorluk olarak ortaya çıkmıştır.

Bu bağlamda bilgi manipülasyonları siyasi istikrarı, kamu güvenliğini ve diplomatik ilişkileri etkileyen önemli bir zorluk olarak ortaya çıkmaktadır. Bunlara ek olarak yanlış ve yanıltıcı bilgilerin tüm biçimleri aynı özelliklere, niyetlere veya sonuçlara sahip değildir. Bu sebeple dezenformasyon ve dijital güvenlik arasındaki ilişkiyi doğru şekilde analiz etmek için çeşitli kavramlar arasındaki ayrımların yapılması gerekir. Bu noktada dezenformasyon (disinformation), yanlış bilgilendirme (misinformation) ve kötü amaçlı bilgilendirme (malinformation) şeklinde üç bilgi bozukluğu kavramı karşımıza çıkmaktadır. Bu kavramlar bilgi bozukluklarının farklı biçimlerini gösterir ve çağdaş dijital tehditleri ve stratejilerini anlamak için önemli bir kavramsal çerçeve oluşturur.

İlk olarak dezenformasyon (disinformation) kavramı, bireyleri, grupları, kurumları ve kuruluşları manipüle etmek veya onlara zarar vermek amacıyla kasıtlı olarak yanlış veya yanıltıcı bilgilerin yayılması olarak tanımlanabilir (Wardle & Derakhshan, 2017, s. 20). Ancak siber güvenlik açısından bakıldığında, belirli bir bilginin tamamen yanlış mı yoksa sadece yanıltıcı mı olduğu sorusu genelde ilk aşamada önemli değildir. Daha önemli olan

nokta, kurumların faaliyetlerine, itibarlarına veya istikrarlarına zarar vermek amacıyla tasarlanmış bilgi faaliyetlerine karşı geliştirdikleri önleme ve bunlara yanıt verme kapasiteleridir (Boevink, Mok, & M.Int, 2023, s. 6). Bu noktada önemli örneklerden biri 2016 Amerika Birleşik Devletleri başkanlık seçimleri sürecidir. Rus devlet bağlantılı aktörlerin seçim süreçlerini etkilemek ve demokratik kurumlara olan kamu güvenini zayıflatmak amacıyla sosyal medya platformları üzerinden dezenformasyon kampanyaları yürüttükleri belirlenmiştir. Bu dezenformasyon sürecinde kutuplaştırıcı ve yanıltıcı bilgiler yayılarak bu tür operasyonların dijital platformlar aracılığıyla nasıl siyasi müdahale ve stratejik etki araçları olarak kullanılabileceği görülmüştür (U.S Senate Intel Committee, 2019).

İkinci olarak yanlış bilgilendirme (misinformation), kasıtlı olarak zarar verme veya kitleleri manipüle etme amacı olmaksızın paylaşılan yanlış veya hatalı bilgileri ifade eder. Bu durumlarda aktörler doğru veya güvenilir olduğuna inanarak yanıltıcı içerik yayabilirler (Wardle & Derakhshan, 2017, s. 20). Yakın bir örnek olan COVID-19 pandemisi, yanlış bilgilendirme kavramı temelinde yanlış ve yanıltıcı bilgilerin yayılarak halk sağlığı ve toplumsal güvenlik açısından önemli zorlukların ortaya çıktığı önemli bir örnektir. Virüsün kökeni, tedavi yöntemleri, aşılar ve önleyici tedbirler hakkındaki iddialar halk arasında büyük bilgi düzensizliğine yol açtı ve resmi sağlık kurumlarının bilgileri ile uyumsuzluklar ortaya çıktığı görüldü. Sağlık konusundaki yanlış bilgilerin hızla yayılması ve teyit edilmesinin güçlüğü, insanla arasında sadece belirsizlik ve kaygıları arttırmakla kalmayarak bazı durumlarda hastalığın yayılmasına doğrudan sebep olduğu görülmüştür. Bu nedenle pandemi, dijital ortamdaki dezenformasyonun bir iletişim sorununun ötesine geçerek kamu güvenliği ve kurumsal güveni etkileyen geniş bir güvenlik tehdidine nasıl dönüşebileceğini göstermiştir. Ek olarak bu süreç sosyal medya platformlarındaki içerik denetleme mekanizmalarının zayıflıklarını da göz önüne çıkarmıştır (Hsu, 2022).

Buna karşılık olarak üçüncü kavram kötü niyetli bilgilendirme (malinformation), gerçeğe dayanan ancak bireylere, kuruluşlara veya devletlere zarar vermek amacıyla kasıtlı olarak üretilen ve kullanılan bilgileri ifade eder. Bu bilgi bozukluğu biçimi genellikle siyasi, sosyal veya itibar zedelenmesi amaçlı olarak gerçek bilgilerin stratejik anlamda ifşa edilmesini, manipüle edilmesini veya çarpıtılmasını içermektedir (Wardle & Derakhshan, 2017, s. 20). 2012 yılında LinkedIn şirketinin yaşamış olduğu büyük veri ihlali olayı, milyonlarca kullanıcının şifre ve hesap bilgilerinin ifşa edilmesine yol açarak önemli bir örnek olmuştur. Bu olayın ardından birçok kullanıcı, kişisel bilgilerini ele geçiren kötü niyetli kişilere fidye

ödemesi yapılmadığı takdirde hesap bilgilerinin kötüye kullanılması tehdidi ile karşı karşıya kalmışlardır. Birkaç yıl sonra çalınan bilgilerin deepweb pazarında satıldığını gösteren raporlar ortaya çıkmış ve bu durum büyük ölçekli veri ihlallerinin uzun vadeli güvenlik sorununun etkilerini ortaya koymuştur. (Krebs, 2016).

2023 yılında yayınlanan Birleşmiş Milletler (BM) Dijital Platformlarda Bilgi Bütünlüğü raporunda bilgi bütünlüğünün korunması ve dezenformasyonla mücadele edilmesi uluslararası toplum için acil bir öncelik olarak belirtilmiştir. Raporda dezenformasyon ve türlerinin dijital alanın ötesine uzandığı ve kamu güveni, demokratik yönetişim ve barış gibi alanları etkileyen çok boyutlu riskleri barındırdığı vurgulanmıştır (UN, 2023, s. 25). Görüldüğü üzere dijital ortamlarda giderek yaygınlaşan dezenformasyon, yanlış bilgilendirme ve kötü niyetli bilgilendirme faaliyetleri, bilginin siyasi, sosyal ve güvenlik dinamiklerini etkileyen stratejik bir araç haline geldiğini göstermektedir. Dijital iletişim teknolojileri bilginin sınırlar ötesinde hızlı bir şekilde yayılıp manipüle edilmesini mümkün kılarken aynı zamanda bilgi de devlet ve devlet dışı aktörler arasındaki çekişmenin merkezi bir alanı haline gelmiştir. Bu bağlamda bilginin siyasi etkileme ve toplumsal manipülasyon için stratejik kullanımı çağdaş uluslararası ilişkilerde geniş bir anlama sahip olan bilgi savaşı ile de yakından ilgili olduğu söylenebilir.

Bilgi savaşı, bilişsel savaş (cognitive warfare) ve hibrit savaş (hybrid warfare) ile açıklanabilecek çok yönlü bir stratejik alan olarak görülebilir. İnsan zihnine yönelen bilişsel kısım ile devlet stratejileri içerisindeki yeri hibrit bir savaş alanı ile ilişkilendirilebilir. Bu bağlamda bilginin yalnızca iletişim aracı olarak değil stratejik bir çatışma alanı olarak kabul edilmesi mümkündür. Bilginin bir savaşın parçasına dönüşmesi sürecinde dijital iletişim sistemlerine olan bağımlılığın artması, bilgiyi siyasi bilişsel algıları, kamuoyu ve devlet davranışlarını etkileyebilecek stratejik bir araca dönüştürdüğü görülmektedir (Marangione, 2021, s. 151).

Dezenformasyonun tek başına hareket etmediği, daha geniş hibrit stratejiler ağının bir parçası olduğunu söylemek mümkündür. Bu bağlamda bilişsel savaş alanı önemli bir kavram olarak karşımıza çıkmaktadır. Bilişsel savaş, genel olarak bir düşmanın algısını hedefini zayıflatmak, etkilemek veya etkisiz hale getirmek amacıyla manipüle etmek amacıyla tanımlanabilir. NATO (North Atlantic Treaty Organization) bilişsel savaşı, bilişsel üstünlük için verilen bir mücadele olarak kavramsallaştırmıştır. Bu mücadele, bilişsel bir avantaj elde etmek ve korumak için tasarlanmış koordineli bir askeri ve sivil faaliyetleri içerir. Bu savaş biçiminin en önemli amacı ise karar alma süreçlerini şekillendirmek ve manipüle etmek için mevcut tüm

bilgi, strateji ve araçları kullanarak bilişsel yollarla insan davranışlarını etkilemektir (Blatny & Søndergaard, 2025, s. 6-7). Bilişsel savaş, bilginin silahlandırılmasına ve kamu güveninin kasıtlı olarak manipüle edilmesine dayandırılmıştır. Düşman aktörler propaganda, dezenformasyon ve deepfake gibi teknolojiler aracılığıyla siyasi süreçleri etkilemeyi ve kamuoyu algısını şekillendirmeyi amaçlamaktadır. Bu bağlamda koordineli bilgi operasyonları yoluyla bilişsel zaaflar kullanılarak bireylerin algıları hedef alınmaktadır (Blatny & Søndergaard, 2025, s. 13-14). Görüldüğü üzere modern çatışmalar artık insanların düşünme süreçlerini hedef almaktadır. Bu bağlamda insan zihninin çatışma alanı haline geldiğini ve dezenformasyonun bilişsel savaşta kullanılan temel silahlardan biri olduğunu söylemek mümkündür. Özellikle dijital platformlar üzerinden toplumun düşünme biçimleri, karar alma süreçleri ve algıları hedef alınmaktadır. Bilişsel savaşın bu önemli ve geleneksel olmayan çatışma süreçleri toplumsal güveni, seçim süreçlerini ve kurumlara güveni azaltarak güvenlik boyutunda yeni boyutların kapılarını açmaktadır.

Öte yandan hibrit savaş ile dezenformasyonun arasında doğrudan ve tamamlayıcı bir ilişki bulunmaktadır. Dezenformasyon, modern hibrit tehditlerin en temel araçlarından biri olarak kullanılmaktadır. Hibrit savaş, devlet veya devlet dışı aktörler tarafından belirli siyasi hedeflere ulaşmak için askeri veya askeri olmayan, geleneksel veya geleneksel olmayan çeşitli yöntemlerin koordineli kullanımı olarak açıklanabilir. Bu bağlamda aynı stratejik amaçlar çerçevesinde yürütülen siber saldırılar, kimyasal saldırılar ve dezenformasyon faaliyetleri bu kapsamın içine girmektedir (EEAS, 2018). Bu bağlamda dezenformasyonun toplumları istikrarsızlaştırmak, zayıflatmak veya siyasi bağlamda karar alma süreçlerini etkileyen karşılıklıkları yaratmayı amaçlayan hibrit savaş bileşenlerinden önemli bir tanesi olduğunu söylemek mümkündür.

Görüldüğü üzere dezenformasyon ve güvenlik arasındaki ilişki, günümüz uluslararası güvenlik ortamında daha önemli ve karmaşık bir hale gelmiştir. Dijital iletişim teknolojilerinin gelişimi sadece bilgi üretimi ve dolaşımını dönüştürmekle kalmamış aynı zamanda bilgi manipülasyonları ve siber alanda gerçekleştirilen yeni güvenlik açıkları da yaratmıştır. Bu bağlamda dezenformasyon iletişim ile ilgili bir kavramdan öteye evrilerek çok boyutlu bir dijital güvenlik sorunu haline gelmiştir. Bilgi savaşı, bilişsel savaş ve hibrit savaş tehditlerinin artan kullanımı da siber alanda işlenen bilgilerin stratejik önemini arttırmıştır. Bu nedenle dezenformasyon ve dijital güvenlik arasındaki etkileşimin, çağdaş güvenlik tehditleri

temelinde hem teknolojik hem de bilişsel boyutlarını kapsayan daha geniş bir çerçeveye sahip olduğu görülmektedir.

Dezenformasyonun Siber Güvenlik Tehdidi Olarak Kavramsallaştırılması

Dezenformasyonun, sadece dar kapsamlı bir iletişim ve bilgi temelli bir sorun olarak değil, aynı zamanda siyasi istikrarı, kurumsal güveni ve demokratik sistemi etkileyen çok boyutlu bir dijital güvenlik tehdidi olarak anlaşılması önemli bir noktadır. Bu bağlamda dezenformasyonun klasik anlamda donanım ve yazılım çökertmeyi hedefleyen siber operasyonların ötesinde, dijital ağlar ve ileri seviye teknolojilerle entegre edilmiş geniş çaplı bir bilişsel güvenlik tehdidi olduğunu söylemek mümkündür.

Dezenformasyon, hedef kitleleri aldatmak ve algıları, davranışları veya siyasi sonuçları etkilemek amacıyla bilginin kasıtlı şekilde manipüle edilmesi anlamına gelirken, benzer şekilde siber tehditler de genellikle hedef alınan sistemlere, kurumlara veya toplumlara zarar vermek amacıyla belirli saldırı çeşitleri aracılığıyla gerçekleştirilen kasıtlı eylemler olarak tanımlanabilir. Bu açıdan bakıldığında dezenformasyon kampanyaları, organize olmuş aktörler, stratejik hedefler, hedef seçimleri ve amaçlanan etki de dahil olmak üzere siber tehditlerle ilişkili benzer yapısal özelliklere sahiptir (Caramancion, Li, Dubois, & Jung, 2022, s. 3-4). Bu bağlamda epistemolojik olarak bakıldığında dezenformasyon ve siber tehditlerin birbirleri ile uyumlu bir kavramsal çerçeve içerisinde oldukları görülmektedir. Bu durum aynı zamanda dezenformasyonun yalnızca iletişimle ilgili bir olgu olmaktan ziyade çok boyutlu bir dijital güvenlik tehdidi olarak anlaşılmasını güçlendirmektedir.

Dezenformasyon, manipüle edilmiş bilgiler ve deepfake gibi teknolojiler kullanarak insan zihnindeki bilişsel zaafları, önyargıları ve mantıksal hataları olumsuz manada kullanmayı hedeflemektedir (Jaiman, 2021). Başka bir değişle geleneksel siber saldırılar teknolojik sistemleri alt etmek için kullanılırken dezenformasyon insan düşüncelerini ve algılarını doğrudan etkilemek için teknolojiyi kullanmaktadır (Boevink, Mok, & M.Int, 2023, s. 7). Bu durum literatürde bilişsel hackleme (cognitive hacking) olarak adlandırılmıştır ve siber güvenliğin doğrudan insan zihnine yöneltilmiş bir boyutu olarak ele alınmıştır (Bone, 2018). Bilişsel hackleme genellikle meşru bilgi kaynaklarına benzeyen, tasarlanmış aldatıcı içerikler aracılığıyla mevcut inançları güçlendirmeyi veya bireylerin gerçeklik algılarını çarpıtmayı amaçlamaktadır. Bilişsel süreçlere yapılan bu müdahale, kamuoyu, davranış ve karar alma süreçlerini etkileyerek bazı durumlarda kritik altyapılara yönelik doğrudan yapılan siber

saldırıların etkisinden daha büyük sonuçlar doğurabilir. Ortaya çıkan bilgi karmaşası ve gerçekler arasındaki belirsizlik kurumsal güvenilirliği zayıflatabilir ve toplum işleyişini aksatabilir (Caramancion, Li, Dubois, & Jung, 2022, s. 1-2).

Görüldüğü üzere dezenformasyon ile siber saldırı arasındaki farklardan en önemlisi hedeftir. Fakat eylemler, stratejiler ve zararlar büyük oranda benzerlik göstermektedir. Örneğin kötü niyetli aktörlerin sahte haberlerle dijital platformlarda gerçekleri perdelemeleri veya yanlış iletmeleri, siber güvenlikteki sunucuları kitleme hedefinde olan DDoS saldırıları ile aynı mantığa dayanmaktadır. Benzer şekilde insanların bilişsel düzeyde duygularını manipüle etmek, bir siber saldırı yöntemi olan oltalama saldırılarının temel motivasyonları büyük bir benzerlik göstermektedir (Jaiman, 2021). Her iki saldırı biçimi de hedeflerine ulaşmak için bireylerin teknolojiye, dijital platformlara ve tanıdık arayüzlere olan güvenlerini istismar etmektedir. Buna ek olarak siber alandaki kimlik ağı operasyonları genellikle finansal kazanç veya veri hırsızlığı gibi amaçlarla gerçekleştirilirken bilişsel saldırılar yoluyla yayılan dezenformasyon faaliyetleri ise kamuoyu manipülasyonu, sosyal kutuplaşmanın yaratılması, seçim süreçlerine müdahale ve siber savaş stratejilerinin geliştirilmesi gibi daha geniş stratejik hedeflere sahiptir. (Caramancion, Li, Dubois, & Jung, 2022, s. 14).

Dezenformasyonun dolaşım sağladığı sosyal medya platformlarının yapısal özellikleri, dezenformasyonun temel dijital altyapısını oluşturmaktadır. Bu platformlar, kullanıcı davranışlarını analiz eden makine öğrenmesi algoritmaları ile içerik dağıtımını gerçekleştirir. Faaliyetler genellikle bot ağları, sahte hesaplar, koordineli manipülasyon stratejileri ve deepfake teknolojileri gibi birbirine bağlı mekanizmalara dayanmaktadır. İnsan davranışlarını taklit edebilen sistemler aracılığıyla bot ağları yapay olarak etkileşim yaratır ve seçilen anlatıları güçlendirerek kamu etkileşimi görünümü oluşturur (Aras, 2026, s. 165-166).

Özellikle seçim dönemlerinde bot hesaplar ve sahte sosyal medya profilleri, propaganda içeriklerini yaymak ve dezenformasyon kampanyalarını yürütmek için kullanılmaktadır. Belirli siyasi aktörleri destekleyen veya hedef alan içerikler sistematik olarak yayılır ve siyasi söylemler yapay olarak şekillendirilmektedir. Bu uygulamalar, dijital ortamlarda kamuoyunun gerçekliğini bozar ve siyasi kutuplaşma yaratarak demokratik süreçlerin manipülasyonunu kolaylaştırmaktadır. Bu bağlamda algoritmik olarak yönlendirilen dezenformasyon kampanyaları dijital platformların nasıl siyasi etki ve algı yönetimi araçlarına dönüştürülebileceğini göstermektedir.

Siber Destekli Dezenformasyon

Siber destekli dezenformasyon, belirlenen hedefe ulaşmak için bilgi ortamını değiştirmeyi veya bulanıklaştırmayı amaçlamaktadır. Amacı, karar vericilerin algılarını etkilemek ve karar aşma süreçlerinde mevcut bilgiler konusunda belirsizlik yaratmaktadır. Güvenilir veya güvenilmez bilgiler arasındaki ayrım bulanıklaşır ve dezenformasyon olayların değerlendirilmesini zorlaştırır. Bu bağlamda bilgi karmaşasının yaratılması karar vericilerin sorunları etkili şekilde değerlendirme süreçlerini etkilemektedir. Gerçek bilgiler konusunda fikir birliği sağlansa bile medya organları veya diğer kaynaklar aracılığıyla dolaşıma sokulan bilgilerin manipüle edilmiş olabileceği algısı, bilgi ekosistemine olan güveni zedeleyebilmektedir (Baştan & Oran, 2024, s. 1214-1215).

Çağdaş çalışmalar devletlerin stratejik hedeflerine yalnızca geleneksel askeri yeteneklerle değil aynı zamanda bilgi ortamının kontrolü ve manipülasyonu yoluyla da ulaşmaya çalıştığını göstermektedir. Bu bağlamda çevrimiçi alanda dijital platformlar aracılığıyla yürütülen bilgi operasyonları, dezenformasyon kampanyaları ve siber destekli iletişim stratejileri devlet yönetiminin önemli araçları haline gelmiştir (Jabrailov, 2025, s. 716).

Demokratik süreçlere yönelik en bilinen dijital müdahalelerden biri olan Cambridge Analytica skandalı, dijital manipülasyon ve siyasi dezenformasyon arasındaki ilişkiyi seçim süreçlerinde gösteren önemli örneklerden biri olarak karşımıza çıkmaktadır. 2016 Amerika Birleşik Devletleri (ABD) başkanlık seçimleri ve Brexit kampanyası sırasında, Cambridge Analytica'nın milyonlarca Facebook kullanıcısının kişisel verilerini izinsiz olarak topladığı ve bu bilgileri seçmen profili oluşturmak ve siyasi mesajlar iletmek için kullandığı tespit edildi. Bu skandal, eski şirket çalışanının firmanın bireylerin psikolojik kırılganlıklarını ve davranışsal eğilimlerini kullanmak üzere tasarlanmış algoritmalar geliştirdiğini ve bunun sonucunda kullanıcıları etkileyen büyük ölçekli veri gizliliği ihlallerine yol açtığını açıklamasıyla uluslararası gündemde dikkat çekmiştir. Bu olay ayrıca dijital veri analitiğinin ve algoritmik hedeflemenin modern siyasi kampanya stratejilerini nasıl şekillendirdiğini göstermiştir (Persily, 2017, s. 65-66).

Organize sosyal medya manipülasyonu faaliyetlerinde en öne çıkan örneklerden biri ise Rusya'nın ''troll fabrikası'' olarak bilinen İnternet Araştırma Ajansıdır (IRA) (McCombie, Uhlmann, & Morrison, 2020, s. 97-98). Rus siyasileri ve istihbarat yapıları ile bağlantılı olduğu iddia edilen bu yapının faaliyetleri, dijital ortamlarda gerçek kamuoyu katılımını

simüle etmek için tasarlanmış koordineli ve kurumsallaşmış yöntemlere dayanmaktadır. Çalışanların gerçek bir siyasi tartışma görünümü yaratmak için büyük miktarda çevrimiçi içerik ürettikleri, farklı aktörlerin kasıtlı olarak karşıt görüşleri benimseyerek bölücü anlatıları güçlendirdikleri ve kamuoyu algısını manipüle ettikleri tartışmalar arasında yer almaktadır. Ayrıca güvenilirlik ve meşruiyet oluşturmak için sahte hesapların uzun vadede geliştirildiği bilinmektedir (Aras, 2026, s. 168). Bu troll fabrikasının gelişmişliği özellikle 2016 ABD başkanlık seçimlerine Rus müdahalesine ilişkin soruşturmalar sırasında belirgin hale gelmiştir. Miller'in (2019) çalışmasına göre, IRA ile bağlantılı olduğu belirlenen 3.814 Twitter hesabından paylaşılan 200.000 tweet üzerinde araştırma yapılmıştır. Bu araştırma, Rus dezenformasyon kampanyalarına yerleştirilmiş manipülasyon stratejilerinin analiz edilmesini sağlamış ve çağdaş bilgi savaşında dijital propaganda ve algı yönetiminin stratejik kullanımını göstermiştir.

Görüldüğü üzere dezenformasyonun dijital altyapısı seçim güvenliğini yalnızca fiziksel sandık güvenliği olmaktan çıkarıp bilişsel ve algısal bir güvenlik meselesine dönüştürmüştür. Dijital dezenformasyon, seçmen davranışlarını manipüle etmek, siyasi rakipleri itibarsızlaştırmak ve demokratik süreçlere olan güveni sarsmak için sistematik bir silah olarak kullanılmaktadır. Bu tür operasyonların amacı, tek bir doğru oluşturmak veya bunu dayatmak değil, siyasi ve sosyal gerçeklikler konusunda belirsizlik, güvensizlik ve kutuplaşma yaratarak bilgi ortamının kendisinin istikrarsızlaştırılması olarak ifade edilebilir.

Dezenformasyonun Stratejik ve Diplomatik İşlevi

Diplomasinin Dönüşümü

Dijital çağda dezenformasyon, uluslararası ilişkilerde ve diplomaside stratejik bir silah ve hibrit savaşın temel unsurlarından biri haline gelmiştir. Geleneksel savaşların aksine günümüzde devletlere veya kurumlara zarar vermek için fiziksel sunucular veya sınır ötesi operasyonlardan ziyade toplumun yapısına, kurumların itibarına ve algılara zarar vermek yeterli olabilmektedir. Dezenformasyon ve diplomatik ilişkiler arasındaki bağlantının, bilginin stratejik bir silah olarak görülmesi ve devletlerin dış politika hedeflerine ulaşmak için siber alanı bir savaş alanı olarak kullanması zemininde şekillendiği söylenebilir. Bu noktada kamu diplomasisi, dijital diplomasi, siber diplomasi ve stratejik iletişim kavramları önemlidir.

Kamu diplomasisi, 1960'larda kitle iletişim teknolojilerinin gelişimi ve siyaset üzerindeki etkisiyle birlikte ayrı bir diplomasi yöntemi olarak ortaya çıkmıştır. Devletlerarası ilişkilerden farklı olarak kamu diplomasisi devletler ve toplumsal arasındaki iletişim süreçlerine ve toplumların kendi aralarındaki etkileşimlerine dayanmaktadır. Bu noktada kamu diplomasisi, devletlerin kitle iletişim araçlarıyla yabancı kamuoyunu etkilemelerini ve onlarla iletişim kurmalarını amaçladıkları stratejilerini ifade etmektedir (Ekşi, 2022a, s. 6). Bilgi ve iletişim teknolojilerinin hızlı gelişimi, kamu diplomasisinin yapısını, yöntemlerini ve kapsamını önemli ölçüde dönüştürmüştür. Dijitalleşme hızlanırken diplomatik uygulamalar da geleneksel iletişim kanallarının ötesine geçerek teknolojik gelişmeler ve değişen küresel siyasi dinamikler temelinde yeniden şekillenmeye devam etmiştir. Bu süreçte dijital diplomasi, siber diplomasi, sosyal medya diplomasisi gibi kavramlar ortaya çıkmıştır. Kavramsal farklılıklara rağmen bu yaklaşımlar temelde giderek birbirine daha fazla bağlanan dijital ortamlarda faaliyet gösteren kamu diplomasisinin çeşitli boyutlarını temsil ettiği söylenebilir (Ekşi, 2022b, s. 36-37).

Dijital diplomasi ve siber diplomasi kavramları birbirleri ile karıştırılsa da temelde ayrılırlar. Dijital diplomasi kavramı genel olarak diplomatik faaliyetlerin yürütülmesinde dijital teknolojilerin kullanımını ifade ederken siber diplomasi ise siber alanda ortaya çıkan sorunları ve çatışmaları ele almak için diplomatik mekanizmaların ve süreçlerin kullanımı ile ilgilidir (Riodan, 2016). Bu bağlamda dijital diplomasinin diplomatik uygulamaların dijitalleşmesine odaklandığı, siber diplomasinin ise öncelikle siber güvenlik ile ilgili siber alanda devletlerarası iş birliğine odaklandığı söylenebilir.

Modern dijital teknolojiler ve sosyal medya araçları uluslararası diplomaside yaygınlaşsa bile dijital diplomasi geleneksel diplomasinin bir alternatifi olarak görülemez (Alethawy, 2022, s. 82). Dijital diplomasi geleneksel diplomasinin yerini almaktan ziyada onun hedeflerini daha hızlı ve az maliyetli şekilde gerçekleştiren kullanışlı bir uzantısı ile tamamlayıcı olarak işlev görmektedir (Alethawy, 2022, s. 87).

Uluslararası ilişkilerde dijital diplomasinin gelişmesi, devletlerin dijital platformlar üzerinden eş zamanlı olarak diyalog halinde olmalarını sağlamaktadır. Bu sanal ortamda üretilen bilgilerin diplomasi üzerindeki etkisi sadece teknolojik bir gelişme olarak görülmemelidir. Bu durum aynı zamanda küresel olarak gücün nasıl kullanıldığının da bir dönüşümü olarak yorumlanmalıdır (Jabrailov, 2025, s. 718) Siber alanda gerçekleştirilen bu diplomasi süreci, siber alanın doğası gereği çeşitli riskleri de barındırmaktadır. Dijital diplomasinin

yaygınlaşması, hükümetlerin siber güvenlik politikalarını da doğrudan etkilemektedir. Hükümetlerin çevrimiçi ağlardaki resmi kurum verilerinin, diplomatların iletişim trafiğinin ve dijital varlıklarının güvenliği büyük bir zorunluluk olarak karşımıza çıkmaktadır. Bu doğrultuda devletlerin dijital diplomasinin yaratmış olduğu bu yeni etkileşim alanını korumak ve sağlıklı işleyebilmek için ulusal düzeyde savunma güçlerini arttırmaları gerekmektedir. Çünkü dijital diplomasi yoluyla geleneksel anlamda ulaşılamayan olumlu ve olumsuz gelişmeler uluslararası arenayı kolaylıkla etkileyebilmektedir.

Bu kolay etkileşim ve erişilebilirlik alanı, iletişim ve bilgi paylaşımı için sınırsız bir bilgi kirliliğine sebep olmaktadır. Böyle bir ortamda güvenilir kaynakların belirlenmesi ve gerçek bilgilerin yanlış bilgilerden ayırt edilmesi zorlaşmaktadır. Bu bağlamda sosyal medya yerleşik medya kurumlarının bilgi denetleme rolünü zayıflatmaktadır. Bireyler geniş kitlelere ulaşabilir ve yüksek etkileşimli içerikler sayesinde kamuoyunu şekillendirebilir. Bu bağlamda dezenformasyon, kullanılabilecek önemli bir güçtür. Geleneksel diplomasinin tıkandığı veya doğrudan askeri çatışmanın yapılmadığı durumlarda devletler bu geniş bilgi ağı içerisinde dezenformasyonu hibrit savaşın ve psikolojik operasyonların merkezine yerleştirebilir (Aras, 2026, s. 165-166). Dijital diplomasi, devletlerin dış politika hedefleri çerçevesinde uluslararası prestij kazanmak ve yumuşak güç oluşturmak için dijital kanalları kullanması olduğu için bu noktada dezenformasyon ise bu durumu tersine çevirerek aynı dijital kanalları yalan ve manipülatif bilgi yaymak için kullanmaktır. Bu bağlamda dezenformasyon yanlışlıkla yapılan bir hatadan ziyade rakipleri zayıflatmak ve uluslararası müzakereleri manipüle etmek için kasten tasarlanmış diplomatik bir silah olarak karşımıza çıkmaktadır (NextGen Diplomat, 2026). Bu bağlamda dijital diplomasi, sadece bir dış politika temelinde iletişim veya tanıtım aracı olarak değil, devletlerin bilgi operasyonları yapabildiği ve dezenformasyonu kolaylıkla yayabildiği bir alan olarak yorumlanabilir.

Dezenformasyon ve Diplomatik Meşruiyet Mücadeleleri

Dijital iletişim teknolojilerinin gelişimiyle uluslararası arenanın aktörleri kamuoyu algısını şekillendirmek ve siyasi sonuçları etkilemek için giderek daha fazla rekabet içerisine girerken bilgi ortamları jeopolitik çatışmaların da önemli bir alanı olarak ortaya çıkmıştır. Bu bağlamda dezenformasyon sadece yanlış bilginin yayılmasıyla sınırlı görülmemelidir. Aksine dezenformasyon siyasi meşruiyeti inşa etmek, güçlendirmek veya zayıflatmak için kullanılabilecek stratejik bir araçtır. Anlatıları çeşitli hedefler doğrultusunda şekillendirerek kamuoyunu etkilemek ve gerçeklik algılarını değiştirmek dezenformasyon faaliyetleri

kapsamında değerlendirilebilir. Bu bağlamda bilgi manipülasyonu, diplomatik meşruiyet sağlama, uluslararası güvenilirlik oluşturma ve siyasi etki üzerindeki mücadelelerle ilişkili görülebilir. Bu dinamik yapı, özellikle rekabet eden aktörlerin bilgi operasyonları yoluyla çıkarlarını sağlamaya çalıştıkları küresel çatışmalarda sıklıkla görülmektedir.

Bu noktada yakın dönemde gerçekleşmiş olan Rusya-Ukrayna savaşı, dezenformasyonun diplomatik ve siyasi meşruiyet aracı olarak nasıl kullanılabileceğini göstermektedir. Krizin ilk aşamalarında ABD Dışişleri Bakan Yardımcısı ile ABD Ukrayna Büyükelçisi arasındaki telefon görüşmesinin sosyal medya platformlarına sızdırılması olayı ile siber operasyonlar ve stratejik iletişim arasındaki ilişkinin önemi görülmüştür. Olay, savaş başlamadan önce Rusya'nın Batı'ya güvenilirliği zayıflatmayın amaçladığı ve iletişim ağlarına sızma yeteneklerinin göstermek istemesi olarak yorumlanmıştır (Lange-Ionatamishvili & Svetoka, 2015, s. 107).

Rusya-Ukrayna savaşı boyunca sosyal medya, Rus yanlısı stratejik anlatıların yayılması için önemli bir platform görevi görmüştür. Bu faaliyetler genelde Ukrayna yetkililerinin ve silahlı kuvvetlerinin davranışlarına yönelik olmuştur. Hedef kitleler arasında korku, kızgınlık ve güvensizliği artırmayı ve Ukrayna'nın uluslararası meşruiyetini de zayıflatmayı amaçladıkları iddia edilmektedir (Lange-Ionatamishvili & Svetoka, 2015, s. 108). Bu durum dezenformasyonun günümüz bilgi savaşlarında anlatı oluşturma ve diplomatik etki aracı olarak nasıl kullanılabildiğini göstermektedir.

Rusya-Ukrayna savaşı sırasında bilgi operasyonlarının en belirgin örneklerinden biri Ukrayna'nın Nazilerden kurtarılması anlatısının yayılması olmuştur. Bu anlatının tarihsel yorumlamaların ve siyasi gerçeklerin çarpıtılmasıyla oluşturulduğu ve Rusya'nın Ukrayna'ya yönelik saldırılarını meşrulaştırma amaçlı bir propaganda aracı olduğu iddia edilmiştir. Sosyal medya platformları aracılığıyla yayılan bu anlatılar hem yerel hem de uluslararası kitlelerin algılarını şekillendirmek için kullanılmıştır (Aras, 2026, s. 168).

Sosyal medyada dolaşıma sokulan ve Ukrayna Başkanı Zelensky'nin Ukraynalılara seslendiği video siber alanda gerçekleştirilen dezenformasyonun bir başka örneğidir. Bu videoda Zelensky'nin savaşta başarısız olduklarını ve askerlere silahlarını bırakıp teslim olmaları gerektiğini ilan ettiği görülmektedir. Bu video sonrasında Ukrayna hükümeti yetkilileri kısa süre içerisinde bu videonun deepfake teknolojisi kullanılarak yapılan sahte bir video olduğu,

sosyal medya üzerinden dezenformasyon amaçlı bilinçli bir şekilde dolaşıma sokulduğu ve bu konuda vatandaşları uyardıkları bir uyarı yayınladılar (Burgess, 2022).

Bir diğer önemli dezenformasyon faaliyeti ise biyolojik laboratuvar komplo teorisidir. Pyrra Technologies aslı siber güvenlik şirketi, sosyal medyada işgalden 10 gün önce bir kullanıcının Ukrayna'da ABD'ye ait biyolojik laboratuvar bulunduğunu belirten bir içerik paylaştığını ve bu içeriğin işgal gününden sonra aşırı sağcı sitelerde yüzlerce kez paylaşıldığını belirtmiştir. İşgal günü Twitter'da yine bu teorinin savunulduğu paylaşımlar yapılmıştır. Bunun üzerine Rus yanlısı web sitelerde bu anlatının baskın hale getirildiği belirtilmiştir (Collins & Collier, 2022). Rusya ise bu iddialar çerçevesinde, Ukrayna'nın ABD desteğiyle biyolojik silah laboratuvarına sahip olduğunu iddia ederek Birleşmiş Milletler Güvenlik Konseyi (BMGK)'nin toplanmasını talep etti. BM ve üye ülkeler bu iddiaların tamamen yalan olduğunu belirterek reddettiler. ABD BM Büyükelçisi Greenfield, Rusya'nın bu iddialarına hiçbir kanıt sunamadığını ve bu yalan iddiaların Rusya'nın Ukrayna işgali sırasında kimyasal ve biyolojik silahlar kullanmak için zemin hazırlamasına bir bahane olabileceğinden endişe duyduklarını vurguladı (Landay, Pamuk, & Lewis, 2022).

Yukarıda bahsedilen olaylar, Rusya'nın eylemlerini haklı çıkarma temelinde gerçekleştirdiği dezenformasyon faaliyetlerinden birkaçını göstermektedir. Savaş başlamadan önce Rusya'nın gizli dezenformasyon planları ve Ukrayna işgali için bir ''sahte bayrak operasyonu'' düzenleneceği ABD yetkilileri tarafından kamuoyuna açıklanmış ve Rusya'nın diplomatik alanda işgale gerekçe üretme sebebi engellenmeye çalışılmıştır (BBC, 2022). Fakat Rusya'nın işgalini meşru göstermek ve ABD ve Batı ülkelerinin Ukrayna'ya verdikleri desteği azaltmak için dezenformasyon faaliyetlerine devam ettiği görülmektedir.

BM'nin Mali'de yürüttüğü MINUSMA (Birleşmiş Milletler Mali Çok Boyutlu Entegre İstikrar Misyonu) barış misyonuna yönelik faaliyetler, BM tarafından önemli bir dezenformasyon kampanyası örneği olarak belirtilmiş ve bilgi savaşlarının uluslararası örgütlerin meşruiyetini ve operasyonel kapasitesini hedef alan dezenformasyon faaliyetlerinden biri olduğu vurgulanmıştır. BM'nin 2023 tarihli raporuna göre 2023 yılında Sevare'de gerçekleşen saldırıların ardından sosyal medyada MINUSMA karşıtı manipülatif içeriklerde artış olmuştur. Bu süreçte sosyal medya üzerinden yayılan sahte haberler BM barış misyonuna yönelik güvensizliği arttırmış ve BM personeline yönelik şiddet çağrıları içeren söylemler üretilmiştir. Raporda MINUSMA'nın bu içeriklere karşı sosyal medyada açıklamalar yayınladığı, yayılan yanlış bilgileri düzeltmeye çalıştığı ve şiddet çağrısı içeren

bir videonun kaldırılması için ilgili dijital platform şirketiyle iletişime geçildiği belirtilmiştir. Bu bağlamda BM, barış misyonunun yeniden yapılandırılması kapsamında bilgi operasyonları ve stratejik iletişim kapasitesinin güçlendirilmesini gündeme getirmiştir (UNSC, 2023, s. 7-11). MINUSMA örneği, dezenformasyonun yalnızca kamuoyu algısını etkileyen bir araç olmadığını, aynı zamanda uluslararası örgütlerin sahadaki operasyonel etkinliğini, meşruiyetini ve güvenliğini hedef alabilen bir tehdit aracı olarak kullanılabildiğini göstermektedir. Özellikle sosyal medya platformlarının çatışma alanlarında etki alanına dönüşmesi bilgi güvenliği ile fiziksel güvenlik arasındaki sınırların bulanıklaştığını ortaya koymaktadır.

Sonuç

Dijital iletişim teknolojilerinin hızlı gelişimi ve yayılımı bilginin üretimi, yayılımı ve tüketimini temelden dönüştürmüştür. Bu dönüşüm sürecinde bilgiye erişim kolaylaşmış ve küresel bağlantı güçlenmiş olsa da aynı zamanda bilgi ortamlarının manipülasyonu için de yeni alanlar yaratmıştır. Bu bağlamda bilginin dezenformasyonu iletişimle ilgili bir sorun olmaktan çıkıp siber güvenlik ve uluslararası ilişkiler alanlarında daha önemli bir sorun haline gelmiştir.

Bu çalışmada dezenformasyonun neden bir siber güvenlik tehdidi haline geldiği ve dijital çağda diplomatik süreçleri nasıl etkilediği incelenmiştir. Bulgular, sosyal medya platformlarının, algoritmik güçlendirme mekanizmalarının, veri analizinin ve yapay zekânın entegrasyonunun artmasıyla birlikte dezenformasyon faaliyetlerinin büyük bir ölçekte uygulanmasına olanak sağladığını göstermektedir. Bu noktada dezenformasyonun yalnızca bilgi bütünlüğünü değil aynı zamanda siyasi süreçleri, kamu güvenini ve kurumsal güvenilirlikleri etkileyen bir siber olgu haline geldiğini söylemek mümkündür.

Örneklerde görüldüğü üzere dezenformasyon hem bir güvenlik sorunu hem de stratejik bir araç olarak işlev görmektedir. 2016 ABD Başkanlık seçimleri ve Brexit referandumu örnekleri, dijital ortamda gerçekleştirilen bilgi manipülasyonlarının siyasi süreçleri ve kamuoyunu nasıl etkilediğini ortaya koymaktadır. Rusya-Ukrayna Savaşı ve MINUSMA örneği ise dezenformasyonun stratejik anlatıları şekillendirmek, siyasi meşruiyeti sorgulamak ve uluslararası algıları etkilemek için dijital ortamda kullanılabileceğini göstermektedir. Bu örnekler, jeopolitik rekabetlerin giderek geleneksel askeri ve ekonomik alanların ötesine genişlediğini ve bilgi ortamının alana dahil olduğunu göstermektedir.

Sonuç olarak dezenformasyon, siber güvenlik, stratejik iletişim ve diplomasi kesişiminde yer alan çok boyutlu bir olgu olarak karşımıza çıkmaktadır. Dijital bilgi ortamları siyasi rekabetin merkezi alanları haline geldikçe, bilgi bütünlüğünü koruma ve dezenformasyon faaliyetlerine verilen tepkiler hem ulusal güvenlik hem de uluslararası diplomatik uygulamalar açısından önemi artan bir güvenlik bileşeni oluşturmaya devam edecektir.

Kaynakça

Alethawy, M. (2022). Digital Diplomacy and Cybersecurity. *Ahi Evran Akademi*, 3(1), 82-90.

Aras, H. (2026). Dijital Diplomasiden Siber Saldırıya: Sosyal Medyanın Hibrit Savaş Stratejilerindeki Rolü. *Karadeniz Araştırmaları*, XXIII(89), 161-180.

Bērziņš, J. (2014). Russia's New Generation Warfare in Ukraine: Implications for Defense Policy. *The Journal of Military Operations*, 2(4), 4-7.

Baştan, Y., & Oran, F. Ç. (2024). Rus Dış Politikasında Siber Müdahale Yöntemi Olarak Dezenformasyon Operasyonları. *Yönetim Bilimleri Dergisi*, 22(53), 1205-1230.

BBC. (2022). Russia-Ukraine: US warns of 'false-flag' operation. 15 January, Retrieved from https://www.bbc.com/news/world-europe-59998988 (Accessed Time: 10 May 2026).

Blatny, J. M., & Søndergaard, S. (2025). Cognitive Warfare. NATO Science & Technology Organization. Retrieved from https://www.sto.nato.int/document/cognitive-warfare/ (Accessed Time: 03 May 2026.

Boevink, J., Mok, E., & M.Int, M. P. (2023, Mayıs). How Disinformation Might Hurt Your Business. Compact "Digital Trust: Cyber Security, Privacy & Ethics", Retrieved from https://www.compact.nl/articles/how-disinformation-might-hurt-your-business/ (Accessed Time: 07 April 2026).

Bone, J. (2018, Mart 5). Cognitive Hack: Trust, Deception and Blind Spots. Nisan 2026 tarihinde Corporate Compliance Insights. Retrieved from https://www.corporatecomplianceinsights.com/cognitive-hack-trust-deception-blind-spots/ (Accessed Time: 11 April 2026).

Burgess, S. (2022, Mart 17). Ukraine war: Deepfake video of Zelenskyy telling Ukrainians to 'lay down arms' debunked. Retrieved from https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789 (Accessed Time: 05 May 2026).

Caramancion, K. M. (2020). An Exploration of Disinformation as a Cybersecurity Threat. 2020 3rd International Conference on Information and Computer Technologies (ICICT), (s. 440-444). San Jose, CA, USA. https://doi.org/10.1109/ICICT50521.2020.00076.

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data,* 7(49), 1-18.

Chee, F. Y. (2022, Mart 2). EU bans RT, Sputnik over Ukraine disinformation. Retrieved From https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/ (Accessed Time: 05 May 2026).

Collins, B., & Collier, K. (2022, Mart 14). Russian propaganda on Ukraine's non-existent 'biolabs' boosted by U.S. far right. Retrieved from https://www.nbcnews.com/tech/internet/qanon-ukraine-biolabs-russian-propaganda-efforts-boosted-us-far-right-rcna19392 (Accessed Time: 05 May 2026).

EEAS. (2018, Haziran 13). A Europe that Protects: Countering Hybrid Threats. Retrieved from https://www.eeas.europa.eu/node/46393_en (Accessed Time: 10 May 2026)

Ekşi, M. (2022a). Kamu Diplomasisinde Post-Truth: Bir Meydan Okuma Olarak Dezenformasyon. *İletişim ve Diplomasi,* (9), 3-24.

Ekşi, M. (2022b). Dezenformasyon Çağında Kamu Diplomasisi. *Cihannüma* (11), 36-42.

Hsu, T. (2022, Aralık 28). As Covid-19 Continues to Spread, So Does Misinformation About It. Retrieved from https://www.nytimes.com/2022/12/28/technology/covid-misinformation-online.html (Accessed Time: 12 May 2026).

Jabrailov, M. (2025). Infoimperialism and Security: Cyberattacks, Disinformation, and State Defense Strategies. *Akademik Tarih ve Düşünce Dergisi*, 12(4), 713-724.

Jaiman, A. (2021, Ocak 30). Disinformation Is a Cybersecurity Threat. Retrieved from https://medium.com/swlh/disinformation-is-a-cybersecurity-threat-335681b15b48 (Accessed Time: 25 April 2026).

Krebs, B. (2016, Mayıs 18). As Scope of 2012 Breach Expands, LinkedIn to Again Reset Passwords for Some Users. Retrieved from https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/ (Accessed Time: 24 April 2026).

Landay, J., Pamuk, H., & Lewis, S. (2022, Mart 11). U.N. says no evidence to back Russian claim of Ukraine biological weapons program. Retrieved from https://www.reuters.com/world/un-says-not-aware-any-biological-weapons-program-ukraine-2022-03-11/ (Accessed Time: 16 May 2026).

Lange-Ionatamishvili, E., & Svetoka, S. (2015). Strategic Communications and Social Media in the Russia-Ukraine Conflict. K. Geers içinde, Cyber War in Perspective: Russian Aggression against Ukraine (s. 103-111). Tallinn: NATO CCDCOE Publications.

Marangione, M. S. (2021). Words as Weapons: The 21st Century Information War. *Global Security and Intelligence Studies*, 6(1), 149-187.

McCombie, S., Uhlmann, A. J., & Morrison, S. (2020). The US 2016 presidential election & Russia's troll farms. *Intelligence and National Security*, 35(1), 95-114.

Miller, D. T. (2019). Topics and Emotions in Russian Twitter Propaganda. *First Monday*, 24(5). https://doi.org/10.5210/fm.v24i5.9638.

Milli İstihbarat Akademisi. (2026). Yapay Zekâ Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri. Ankara: *Millî İstihbarat Akademisi.* Retrieved from https://mia.edu.tr/uploads/f/24042026_1.pdf.

NextGen Diplomat. (2026, Mart 7). Disinformation Campaigns Countermeasures: Practical Guidance For Diplomats. Retrieved From https://blog.modeldiplomat.com/disinformation-campaigns-countermeasures (Accessed Time: 10 May 2026).

Nye, J. S. (2002). The Information Revolution and American Soft Power. *Asia-Pacific Review*, 9(1), 60-76.

Nye, J. S. (2019). Protecting Democracy in an Era of Cyber Information War. Cambridge: Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war (Accessed Time: 10 April 2026).

Persily, N. (2017). Can Democraracy Survive The Internet?. *Journal of Democracy*, 28(2), 63-76.

Riodan, S. (2016, Mayıs 12). Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. Retrieved from https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction (Accessed Time: 18 April 2026)

Talinshinsky, E. (2026). Bilgi Savaşının Teorik Temelleri ve Modern Uluslararası İlişkiler Sistemindeki Stratejik Rolü. *Akademik Tarih ve Düşünce Dergisi*, 13(3), 1-11.

U.S Senate Intel Committee. (2019, Ekim 8). Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media. Retrieved from https://www.intelligence.senate.gov/2019/10/08/press-senate-intel-committee-releases-bipartisan-report-russia-e2-80-99s-use-social-media/ (Accessed Time: 13 April 2026).

UN. (2023, Temmuz). Our Common Agenda- Policy Brief 8: Information Integrity on Digital Platforms. Retrieved from https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf (Accessed Time: 05 May 2026).

UNSC. (2023). S/2023/402 Situation in Mali Report of the Secretary-General. Retrieved from https://docs.un.org/en/s/2023/402 (Accessed Time: 10 May 2026).

Wardle, C., & Derakhshan, H. (2017). Informatıon Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Retrieved from https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (Accessed Time: 10 May 2026).