



**Yazar/Author**  
Alp Cenk ARSLAN\*

**Makale Adı/Article Name**

Yeni Güvenlik Konsepti Bağlamında Dezenformasyonla Mücadele

*Combating Disinformation in the Context of New Security Concept*

**ÖZ**

Bu çalışma “iletişimin güvenlik kavramsallaştırması içinde nasıl konumlandığı ve güvenlikle arasındaki ilişkinin mahiyeti” sorunsalı üzerine odaklanmaktadır. Çalışmanın ikincil soruları ise “dezenformasyonun bir güvenlik sorunu olarak teoride nasıl işlenmesi gerektiği”, “dezenformasyon noktasında tehdidin hangi aktörler tarafından karşılanması gerektiği” sorularıdır. Elbette, “neyin / kimin güvenliği” ve “tehditten kimin koruyacağı” da cevaplanması elzem sorulardır. Çalışmanın ana gayesi iletişim alanına dair bir kavram olan dezenformasyon ile güvenliğe yönelik algı ve anlayışları birlikte düşünmek ve sentezlemektir. Çalışmanın temel varsayımı ise dezenformasyonun yalnızca akademik iletişim çalışmaları içerisinde incelenmesinin bütüncül bir bakış açısından uzak düşeceği, bunun yerine bir güvenlik sorunu veçesi de olan dezenformasyonun güvenlik teorileri bağlamında değerlendirilmesi ve çözüm önerilerinin buna göre kurgulanması gerektiğidir. Çalışmada NATO Stratejik İletişim Mükemmeliyet Merkezi, Anadolu Ajansı ve Teyit.org dezenformasyonla mücadele çalışmaları kapsamında değerlendirilmiş, bu üç farklı düzeydeki yapı bütüncül bir güvenlik perspektifinden analiz edilmeye çabalanmıştır. Böylelikle dezenformasyonla mücadele uluslararası örgüt, ulusal haber ajansı ve sivil toplum aktörü veçhelerinden analiz edilmiştir.

**Anahtar Kelimeler:** Yeni Güvenlik Konsepti, Dezenformasyon, Güvenlik Yönetimi, Güvenlik Stratejileri, Güvenlik Teorisi

**ABSTRACT**

This study focuses on the problematic of “how communication is positioned within the conceptualization of security and the nature of its relationship with security”. The secondary questions of the study are “how disinformation should be treated as a security issue in theory” and “which actors should meet the threat of disinformation”. It should be noted that “what/whose security” and “who will protect from threat” are also essential questions. The main aim of the study is to think and synthesize disinformation, a concept related to the field of communication, with perceptions and understandings of security. The basic assumption of the study is that examining disinformation only within academic communication studies would be far from a holistic perspective; instead, disinformation, which also has a security problem aspect, should be evaluated in the context of security theories and solution proposals should be constructed accordingly. NATO StratCom Center of Excellence, Anadolu Agency, and Teyit.org are evaluated in terms of their efforts of combating disinformation within the scope of the study. These bodies from three different levels are analyzed with a holistic security perspective. Thus, combating disinformation is analyzed in the aspects of international organizations, national agencies, and civil society actors.

**Keywords:** New Security Concept, Disinformation, Security Management, Security Strategies, Security Theory

## Extended Abstract

This study delves into the problem of how disinformation is integrated within the framework of new security concept. It explores the nature of the relationship between disinformation campaigns and security framework. The study also raises critical secondary questions such as how disinformation could be theoretically accepted as a security issue and identifies the appropriate actors to counter the threat raising from it. Additionally, fundamental questions such as “whose security” and “who protects from the threat” are addressed within the study. The principle aim is to amalgamate the concept of disinformation with current perceptions and understandings of security. The foundational assumption states that disinformation requires to be analyzed not only within academic communication studies but also within the broader context of security theories to develop comprehensive solutions.

The study begins by developing a theoretical framework that investigates various perceptions of security. Traditionally, security theories have posited the state as the primary reference object. However, this perspective shifted significantly in post-Cold War era, leading to a broader spectrum of security concerns. Modern security understandings have expanded the concept of security to include human, societal, economic, energy, and environmental security. It has moved security away from a solely state-centric focus to a human-centric perspective. This paradigm shift has also redefined the nature of threats, acknowledging non-military threats that have an impact on individual and societal well-being, such as disinformation.

Disinformation is a significant threat to the right to information and psychological health of individuals and societies, which targets both conscious and unconscious aspects. The multifaceted nature of disinformation requires a comprehensive approach to counteract its effects.

Disinformation campaigns are widely recognized as a significant threat in contemporary world, fueled by advancements in information and communication technologies. This complex threat requires a multi-actor and hybrid approach to effectively combat it. The study underlines the necessity for a holistic strategy that involves various actors from diverse backgrounds to address disinformation in a cohesive manner. The emphasis on societal and individual security, including the right to true information and psychological well-being, is crucial within the framework of Türkiye’s new security concept. A comprehensive strategy to combat misinformation must involve coordinated efforts by national and international authorities, as well as civil society organizations.

The incorporation of communication into the conceptualization of security highlights a critical evolution in understanding modern threats. Historically, security has been a state-centric domain, primarily focused on military and territorial integrity. However, the post-Cold War era created a new wave of security concerns that extend beyond traditional boundaries, incorporating non-military dimensions such as economic stability, environmental sustainability, and societal resilience. Disinformation, as a non-military threat, disrupts social cohesion and undermines trust in democratic institutions, making it a critical area of study within security theories.

Disinformation could destabilize civilizations by disseminating false narratives, causing uncertainty, and undermining public trust. As a result, it has a significant impact on security. Misinformation, or the inadvertent distribution of inaccurate information, is not the same as disinformation, which is the intentional spreading of false information. Disinformation is a deliberate strategy employed by variety of actors to manipulate public perception and achieve strategic objectives. This manipulation could occur through different channels, including social media, traditional media, and other communication platforms.

This study investigates various actors involved in combating disinformation: the NATO Strategic Communications Centre of Excellence (StratCom), Anadolu Agency, and Teyit.org, each of which plays a unique role in addressing this issue.

NATO StratCom, established in 2014 in Riga, Latvia, aims at enhancing strategic communication efforts to counter emerging security threats such as disinformation. Even though it operates independently of NATO’s command structure, StratCom supports NATO’s broader communication strategies. Its activities cover policy development, conducting research, and analyzing disinformation campaigns to formulate effective solutions and countermeasures.

NATO StratCom is essential in combating disinformation by leveraging strategic communication tactics to enhance resilience against such threats. The center’s perspective encompasses developing sophisticated communication strategies, conducting detailed analysis of disinformation trends, and facilitating the exchange of best practices among member states. StratCom’s work is crucial in developing a coordinated response to disinformation. It ensures that NATO and its allies remain vigilant and prepared to combat information manipulation.

Founded in 1920, Anadolu Agency has evolved its vision in recent years to include fact-checking, specifically during Türkiye's 2018 Olive Branch Operation into northern part of Syria. The agency engaged in combating disinformation campaigns that targeted the legitimacy of the operation, thereby highlighting the hybrid and multifaceted nature of disinformation. Anadolu Agency's efforts highlight the significance of fact-checking in maintaining the integrity of information disseminated to the public.

Anadolu Agency's fact-checking initiatives during the Olive Branch Operation is an example of the role of national media in countering disinformation. By checking and verifying information and debunking false claims, the agency not only protected the integrity of the operation but also maintained public trust. This proactive approach underlines the necessity for media agencies to build robust fact-checking mechanisms, particularly during times of conflict or crisis when disinformation efforts are most intense.

Established in 2016, Teyit.org is a non-profit fact-checking organization dedicated to verifying suspicious information found on the internet. Its verification process involves scanning for suspicious information, selecting and prioritizing claims, investigating these claims, and publishing the results. Teyit.org's mission extends to enhancing media literacy and critical thinking among internet users, thus empowering the public to understand the accuracy of the information they encounter.

Teyit.org's contribution to combating disinformation is significant. Its contributions is vital particularly in the digital age where information spreads rapidly across online platforms. The organization's methodical perspective to verification, combined with its educational efforts to improve media literacy, empowers individuals to critically assess the information they consume. Teyit.org increases societal resilience against false information and lessens its effects by promoting public awareness.

The study concludes by highlighting the importance of a multi-faceted strategy to combat disinformation, integrating efforts from international organizations, national media, and civil society. The evolving security landscape requires that security theories expand to non-traditional threats like disinformation, ensuring a holistic understanding and effective countermeasures. The coordinated efforts of different actors are essential to safeguard the right to true information and protect the psychological well-being of individuals and societies.

## Giriş

Bu çalışma nitel araştırma yöntemlerinden betimleyici analiz yöntemini kullanarak "iletişimin güvenlik kavramsallaştırması içinde nasıl konumlandığı ve güvenlikle arasındaki ilişkinin mahiyeti" sorunsalı üzerine odaklanmaktadır. Çalışmanın ikincil soruları ise "dezenformasyonun bir güvenlik sorunu olarak teoride nasıl işlenmesi gerektiği", "dezenformasyon noktasında tehdidin hangi aktörler tarafından karşılanması gerektiği" sorularıdır. Elbette, "neyin / kimin güvenliği" ve "tehditten kimin koruyacağı" da cevaplanması elzem sorulardır. Çalışmanın ana gayesi iletişim alanına dair bir kavram olan dezenformasyon ile güvenliğe yönelik algı ve anlayışları birlikte düşünmek ve sentezlemektir. Çalışmanın temel varsayımı ise dezenformasyonun yalnızca akademik iletişim çalışmaları içerisinde incelenmesinin bütüncül bir bakış açısından uzak düşeceği, bunun yerine bir güvenlik sorunu vechesi de olan dezenformasyonun güvenlik teorileri bağlamında değerlendirilmesi gerektiğidir.

Çalışmada öncelikle kuramsal bir çerçeve geliştirilmeye çalışılmış ve bu çerçevede güvenlik algıları incelenmiştir. Geleneksel güvenlik anlayışındaki teoriler güvenliğin referans nesnesi olarak devleti konumlandırması Soğuk Savaş sonrası dönemde değişmiş ve güvenlik çok boyutlu bir hal almıştır. Yeni güvenlik anlayışı olarak özetlenebilecek yeni yaklaşımlar ise güvenliğin referans nesnesini çok daha geniş bir spektrumda ele almış, böylelikle güvenlik tanımı genişlemiş, çeşitlenmiş ve derinleşmiştir. Yeni yaklaşımlar salt askeri güç odaklı tanımlamalar ve kavramsallaştırmalar ve devleti merkeze almak yerine insanın, toplumun, doğanın, enerjinin güvenliği gibi yeni kavramsallaştırmalara gitmişlerdir. Özetle, zaman içerisinde güvenliğin referans nesnesi meta odaklılıktan birey ve toplum odaklılığa doğru ilerlemiştir. Bir başka deyişle, güvenlik insan odaklı bir hale gelmiştir.

Bahsi geçen değişim güvenlik söz konusu olduğunda tehdit tanımlarının da değişimini beraberinde getirmiştir. Bireyin ve toplumun merkeze alındığı bir güvenlik anlayışında tehdidin ne olacağı ve bu tehde karşı kimin / hangi aktörün koruma sağlayacağı soruları doğmuştur. Dezenformasyon söz konusu olduğunda ise bireyin ve dolayısıyla da toplumun haber alma

hakkının ve psikolojik sağlığının tehdit altında olduğu, tehdidin bilince ve bilinçdışına yönelik kurgulandığı görülmektedir.

Birey ve topluma yönelik çok boyutlu bir tehdit olan dezenformasyon, onunla çok boyutlu mücadeleyi gerektirmektedir. Bu çalışmada ele alınan ve doğruluk kontrolü de dahil dezenformasyonla mücadeleyi önceleyen NATO Stratejik İletişim Mükemmeliyet Merkezi, Anadolu Ajansı ve Teyit.org örnekleri mücadelede farklı aktörlerin farklı boyutlarla görev ifa ettiklerini açıklamaktadır. Özetle hibrit bir anlayışa sahip olmak hibrit model içerisinde konumlandırılan dezenformasyonla mücadele için gerekliliğini korumaktadır.

### 1. Kuramsal Çerçeve: Güvenlik Algıları

Geleneksel güvenlik yaklaşımı uluslararası sistemin yapısının anarşi içerisinde olduğunu savunmaktadır. Vestfalya sistemi ulus devlet olgusunun başlangıcı olarak değerlendirilmektedir ve geleneksel güvenlik anlayışı da aynı şekilde bu mihenk taşı kendisi için önemsemektedir. Ulus devletin bir fenomen olarak zihinlere yerleşmesi ve yüzyıllardır kendisini yeniden üretmesi son tahlilde onun fiziksel olduğu kadar algısal olarak da güçlendiğinin, daha da önemlisi merkeze oturduğunun bir göstergesidir. Böylelikle geleneksel güvenlik yaklaşımının temelinde ve merkezinde devlet, dolayısıyla da askeri güvenlik yatmaktadır (Buzan vd., 1998; Ayhan, 2016: 135).

Geleneksel güvenlik yaklaşımının temel boyutları onu daha iyi kavrayabilmek adına incelenmeye ihtiyaç duymaktadır. Bu boyutlar, güvenlikle ilişkili en önemli kavramlardan tehditlerin nedeni, tehditlerin doğası, tehditlere nasıl karşılık verilebileceği, güvenliği kimin sağlamakla yükümlü olduğu ve nelerin güvenliği olarak vurgulanabilmektedir.

Geleneksel güvenlik yaklaşımı ulusal gücü devletin yapabilirlikleri ve kapasitesi ile eş değer görmektedir. Buna göre devlet tehditleri karşılayabilecek düzeyde, bir diğer deyişle yeterli düzeyde ulusal güce sahip olabilmek için her daim askeri gücünü tahkim etmeli ve hazırlıklarını askeri açıdan sürdürmelidir. Geleneksel güvenlik anlayışına göre devletlerin varlıklarını sürdürebilmelerinin ve potansiyel tehditlerle dolu bir dünyada zarar görmemelerinin yegane yolu askeri güçleridir. Geleneksel güvenlik anlayışının ana varsayımlarından birisi de güvenliğin temel amacının toprak, bağımsızlık ve egemenliği korumakla ilintili olmasıdır (Urhal, 2019).

Bu noktada vurgulanmayı hak eden bir diğer konu, geleneksel güvenlik yaklaşımındaki realizm teorisinin yüksek politika olarak askeri politikalar ve alçak politika olarak ise ekonomik politikalar ayrımına gitmesidir. Neorealist teori realist teorisinin temel anlayışını terk etmeden güvenlik yaklaşımına odaklanmakta, ittifaklar kurulması suretiyle uluslararası sistemin güvenliğine vurgu yapmaktadır (Waltz, 1979: 75).

Soğuk savaşın sona erme sürecindeki geleneksel güvenlik anlayışına yönelik eleştiri girişimleri ve soğuk savaşın bitişiyle birlikte ortaya çıkan yeni güvenlik anlayışı güvenlik kavramının çeşitlenmesi, genişlemesi ve derinleşmesiyle sonuçlanmıştır. Buna göre yeni güvenlik kavramsallaştırması güvenliği devleti merkeze alan ve askeri güç temelli yaklaşımı aşarak güvenliğin merkezine daha geniş bir bakış açısı yüklemiştir (Hama, 2017). Güvenliğin referans nesnesinin devletten başka unsurlara kayması bu genişleme ve derinleşmenin ana dinamiklerinden birisini oluşturmuştur. Özellikle Doğu Bloku'nun yıkılmasıyla birlikte güvenlik alanına yeni yaklaşımlar güvenliğin referans nesnelere arasına doğanın, toplumun ve insanın güvenliğini yerleştirmiştir (Ağır, 2015: 102-105; Newman, 2001).

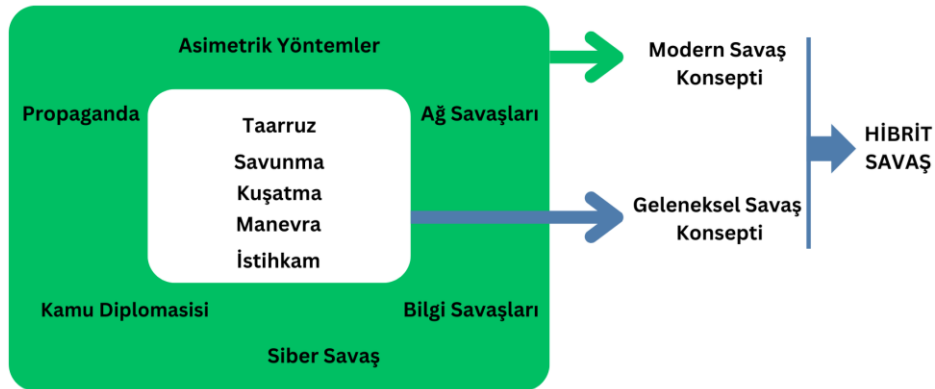
Yeni güvenlik anlayışı içindeki yaklaşımlar geleneksel güvenlik anlayışının askeri tehditleri önceleyen bakış açısını aşmak istemiştir. Yeni güvenlik anlayışına göre tehditlerin kökeni askeri veya devlete dayalı değil aksine devlet dışı ve çok çeşitlidir (Ağır, 2015: 106). Hatta bu tehditler küresel ve uluslararası özelliklere de sahiptir (Hammond-Errey ve Ray, 2019). Her ne kadar realist kökenli yaklaşımlar yeni bakış açılarının bu eleştirilerini güvenliğin tanımlanmamış ve muğlak kalma ile sonuçlanacağını ifade etseler de değişen dünya güvenliğe bakışın çok boyutlu olmasını gerektirmektedir.

Klasik güvenlik anlayışının sorgulanmasına dair en önemli sorular güvenliğin kim ve ne için, nasıl sağlanacağı gibi sorulardır. Özetle, yeni güvenlik anlayışının klasik anlayışa karşı olarak güvenliği yeniden tanımlama çabası güvenliği yalnızca askeri bakış açısından kurtarma yolunda bir çabadır. Özellikle Kopenhag Okulu'ndan Buzan ve Weaver gibi akademisyenler güvenliği çok farklı parametreler ve “sektörler” açısından değerlendirmeye gayret etmektedir (Buzan vd., 1998: 25).

Bu çalışma bağlamından düşünüldüğünde de esas odaklanması gereken nokta güvenliğin referans nesnesinin meta odaklı değil insan odaklı olması gerektiğidir. Zira iletişim ve güvenliğin kesiştiği noktada bir tehdit olarak ortaya çıkan dezenformasyon, bireyin ve dolayısıyla da toplumun güvenliğini, özel olarak ise birey ve toplumun doğru haber alma özgürlüğünün ve psikolojik istikrarının güvenliğini öncelemeyi gerektirmektedir (Arcos vd., 2022). Esasen bu mesele bir bakış açısı meselesi olarak kendisini göstermektedir.

Güvenliğin referans nesnesinin ve ona yönelik kavramsallaştırmaların çok çeşitlendiği bir ortamda hibrit savaş modelinin de çözümlenmesi gerekmektedir. Zira bahsi geçen bir evrende tehditlerin doğası askeri ve askeri olmayan yöntemlerin bir arada kullanımıyla oluşmaktadır. Hibrit model çeşitli doktrinler veya kavramsallaştırmalarla özellikle 1990 sonrası oldukça geniş şekilde tartışılmış bir modeldir. Bu çalışmada değinilen hibrit model, dezenformasyonun bir tehdit olarak haber alma güvenliği, öğrenmenin güvenliğini tehlikeye atan bir olgu olması düşüncesinden yola çıkarak konumlandırılmaktadır. Zira devlet dışı aktörlerin uluslararası sistemde giderek daha görünür hale gelmesi ve tehditlerin boyutunun ve kapsamının değişmesi ona yönelik mücadele anlayışında da bir güncellemeye gidilmesine yönelik ihtiyacı doğurmaktadır. Bugüne dek kavramsallaştırılan hibrit model de tehditlerin çok boyutlu yapısına karşılık çok boyutlu mücadele anlayışını vurgulamaktadır. Günümüzün güvenlik evreninde dolaylı tehditlerin ve savaş yöntemlerinin askeri yöntemlerden daha çok tercih edilmesi söz konusudur. Bunun en temel sebebi ise askeri olmayan teknik ve yöntemlerin maliyetinin az olması ve riskinin düşük olmasından ileri gelmektedir. Bu çalışmanın vaka analizi bölümünde de görüleceği üzere dezenformasyona karşı mücadelede aktörler çok farklı düzeylerden ve arka planlardan gelebilmektedir. Zira dezenformasyonla mücadelenin doğası bu hibrit anlayışı gerekli kılmaktadır (Arcos vd., 2022).

Hibrit anlayış geleneksel ve modern savaş konseptini içinde barındırmaktadır. Buna göre saldırı, savunma, yığınak, kuşatma, manevra ve lojistik gibi geleneksel savaş konseptinin içinde değerlendirilebilecek kavramlar asimetrik yöntemler, network savaşı, kamu diplomasisi, enformasyon savaşı, siber savaş ve propaganda gibi modern savaş yöntemlerinin arkasına saklanmış olarak konumlanmaktadır. Bu sistemleştirmede modern savaş konsepti, geleneksel askeri yöntemlerin kullanılmadığı durumlarda kitlelerin algısını yönlendiren ve manipüle eden yöntemlere karşılık gelmektedir. Burada belirtilmesi gereken en önemli nokta ise günümüzde modern savaş konseptinin gerektirdiği teknolojilere ve bilgiye sahip toplumların daha avantajlı hale gelmesidir (Mumford, 2020: 825).



Şekil 1: Hibrit Savaş Modeli

**Kaynak:** Dedemen, 2016: 165'den esinlenilerek yazar tarafından oluşturulmuştur

## 2. İletişim, Enformasyon ve Güvenlik: Dezenformasyonu Konumlandırmak

Dezenformasyon çağlar boyunca varlık gösteren bir kavram olmasıyla birlikte, tarihte kitle iletişim teknolojileri alanındaki her atılımda boyut atlamış, adeta mutasyona uğramıştır. 19. ve 20. yüzyıllarda kitle iletişim teknolojilerindeki dramatik sıçrayışlar da dezenformasyonun yayılımını ve kitlelerle buluşmasını çok daha kolaylaştırmıştır. Dezenformasyonun kavramsallaştırılmasından önce enformasyon kavramını tanımlamak gerekmektedir. Bu doğrultuda enformasyonun ham veri ve bilgiyle ilişkisini açıklamak da önem arz etmektedir.

Kaynağının kim ve hangi kurum olduğu fark etmeksizin, servis edilen her enformasyonun belirli bir amacı vardır. Bu amaç, bilgi ve enformasyon ile uğraşan kimi kurum için kamusal bir “anlayış” oluşturmak iken bazı kişiler veya kurumlar için manipülasyon ve yönlendirme olarak ortaya çıkmaktadır (Arslan, 2023: 19).

Tanımlamak gerekirse enformasyon kısaca bir konu, kişi ve nesne hakkındaki malumat olarak kavramsallaştırılabilmektedir. Enformasyon, özetle onu algılayan kişi için bir bağlamın içinde anlama sahip uyaran olarak tanımlanmaktadır. Enformasyon bir sistem içerisinde saklandığında veri olarak adlandırılmakta, veri aynı zamanda enformasyonun öncülü de olabilmektedir. Verilerin işlenmesinden sonra ortaya çıkan çıktılar tekrar enformasyon olarak algılanabilmektedir. Enformasyon bir meseleyi kavramak veya eyleme geçmek için kullanıldığında bilgiye dönüşmektedir. Bu haliyle, bilgi daha fonksiyonel mahiyete sahip bir kavram olarak öne çıkmaktadır. Bu noktada enformasyon ve bilgi kavramlarını birbiriyle karıştırmamak gerekmektedir. Örneğin İngilizce “information society” ifadesi Türkçe’ye sıklıkla “bilgi toplumu” olarak tercüme edilmekte ve bir hataya düşülmektedir. Bunun yerine “enformasyon toplumu” ifadesini kullanmak daha isabetli olacaktır. Zira bilgi ve enformasyon aynı anlama gelmeyeceği gibi bu ifadeyle kastedilen anlam “haberleşim ya da malumat toplumu”dur (Cangızbay, 2007: 114). Enformasyonun bir diğer tanımı ise olağan şartlarda doğru bilgi olarak yapılmaktadır (Yayla, 2020: 126).

Diğer yandan, hatalı enformasyon olarak özetlenebilecek misenformasyon kavramı ise dezenformasyonun bir üst kavramı olarak karşımıza çıkmaktadır. Yani dezenformasyon, misenformasyonun alt kavramlarından birisidir. Bu noktada misenformasyon ve dezenformasyon arasında bir ayrıma gidilmekte ve iki kavramın birbirine karıştırılmaması önem arz etmektedir. Misenformasyon, kusurlu haber anlamına gelirken, bilinçdışı yanlışlıklar, hatalar ve göz ardı etmeyle ortaya çıkabilmektedir (Fallis, 2014a: 621).

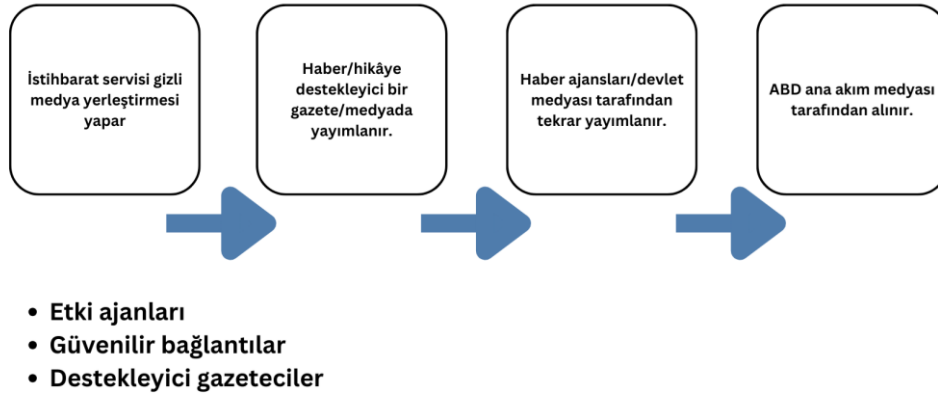
Dezenformasyon ise misenformasyonun tersine yanlış / yalan haberin kasıtlı bir şekilde dolaşıma sokulmasına karşılık gelmektedir. Bilgiyi çarpıtma olarak özetlenebilecek dezenformasyon bilinçli bir şekilde aldatma olarak da tanımlanmaktadır (Fallis, 2014a: 621). Başka bir tanımlamayla dezenformasyon, haberin bilinçli ve sistematik bir şekilde yanlış, uydurma, eksik, çarpıtılmış ve yönlendirilmiş bir biçimde kullanımına karşılık gelmektedir (Yayla, 2020: 126).

Dezenformasyon konusunda öne çıkan bir diğer kavram olan sahte / yalan haber ya da İngilizce meşhur ifadesiyle “fake news” ise kasıtlı ve doğrulanabilir bir biçimde yanlış olan ve okuyucuları yanlış yönlendiren haberleri tanımlamaktadır (Allcot ve Gentzkow, 2017: 211).

Dezenformasyonun bir güvenlik problemi olarak açıklanması 1996 yılında John Arquilla ve David Ronfeldt tarafından yayımlanan “Ağ Savaşı Vukuu” kitabı ve 1998 yılında Koramiral Arthur Cebrowski ve John Garstka’nın kaleme aldıkları “Ağ Merkezli Savaş: Orijini ve Geleceği” makalesinde ortaya çıkmıştır. 2000’li yıllara yaklaşırken yayımlanan bu çalışmalarda iletişim teknolojilerinin savaş evrenine giderek daha çok hakim olacağı, devlet dışı aktörlerden oluşan ağ yapısının yeni bir toplumsal çatışmayı yükselteceği yorumları yapılmıştır (Arquilla ve Ronfeldt, 1996 Akt. Dedemen, 2016: 158). Buna göre 2000’li yıllarla başlayan ve “renkli devrimler” olarak adlandırılan politik süreç dezenformasyon da dahil olmak üzere hibrit savaş modelinin kullanıldığı olaylardır.

Dezenformasyon ve onun güvenlik tehdidi olarak öne çıkışı 20. yüzyılda Sovyetler Birliği'yle ilişkilendirilmektedir. Rusça “dezinformatsiya” ifadesiyle beliren dezenformasyon ABD istihbarat kurumlarının 1950’li yıllardan beri kullandığı bir terim olagelmıştır. Yeni medya teknolojilerinin yükselişe geçtiği günümüzde ise dezenformasyon alabildiğine geniş bir spektrumda kullanılan bir silah halini almıştır. 2016 yılında hakikat sonrası anlamına gelen “post-truth” kelimesinin Oxford sözlüğü tarafından yılın kelimesi olarak seçilmesi de bu durumun bir alametidir (bbc.com, 2016).

Dezenformasyonun hangi yöntemlerle kullanıldığı, onunla mücadele edebilmek için açıklanmayı gerektirmektedir. Bu noktada dört yöntem öne çıkmakta bu yöntemler seçici sansür, arama sıralamalarının (rankings) manipülasyonu, hackleme ve dezenformasyonu direkt yayma olarak sıralanmaktadır (Guess vd., 2018).



Şekil 2: Dezenformasyonun Dolaşımı

**Kaynak:** ABD Savunma Bakanlığı, 2001’den esinlenilerek yazar tarafından uyarlanılmıştır

ABD Savunma Bakanlığı’nın 2001 yılına ait bir el kitapçığı da ABD’de dezenformasyonun hangi yöntemlerle yayıldığına yönelik bazı açıklamalarda bulunmaktadır. Bu sistematığe göre dezenformasyon öncelikli olarak istihbarat servisleri tarafından örtülü şekilde basın kaynaklarına yerleştirilmektedir. Ardından basın kaynaklarına yerleştirilen bu haberler makale ve haber yazısı olarak fikrinsel açıdan yakın medya organlarında yayımlanmaktadır. Sonraki aşamada bu haberlerin yayılması devlet ajansları ve kablolu servisler tarafından yeniden yayına sokulmaktadır. Son aşamada ise bu haberler ABD ana akım medyası tarafından dolaşıma sokulmaktadır. Bu sistematiğe dezenformasyonun yayılmasını hızlandıran aktörler ise etki ajanları, güvenilir bağlantılar ve fikirdaş gazeteciler olarak sıralanmıştır (ABD Savunma Bakanlığı, 2001). Örnek vermek gerekirse 1985 yılında Rus istihbaratı tarafından yürütülen Infektion Operasyonu, HIV virüsü ve AIDS hastalığının ABD tarafından üretilip dünyaya yayıldığı haberini dolaşıma sokma üzerine çalışmıştır. 1992 yılında ise Rus dış istihbarat servisi başkanı Yevgeny Primakov Infektion Operasyonu’nun bir dezenformasyon operasyonu olduğunu kabul etmiştir (Boghardt, 2009: 15).

Yanlış bilginin türleri ise parodi, çarpıtma, taklit, uydurma, hatalı ilişkilendirme, bağlamdan koparma ve manipülasyon olarak sıralanmaktadır. Parodi eğlence ve alaya alma amaçlı hazırlanan, hedef kitleyi yanıltma potansiyeli olan içerikler olarak özetlenebilir. Çarpıtma gerçek anlamından koparıp saptırarak yanlışla sürükleme ve yönlendirmeyi ifade etmektedir. Taklit, kişi ve kurumların taklitleri tarafından dolaşıma sokulan haberlere karşılık gelmektedir. Uydurma, tam anlamıyla üretilmiş ve gerçekle alakası olmayan içeriklere karşılık gelirken hatalı ilişkilendirme ise çeşitli fotoğraf ve görsellerin alakasız vakalarla ilişkilendirilerek sunulmasını ifade etmektedir. Bağlamdan koparma doğru bilgiyi içinde bulunduğu olay örgüsünden kopararak farklı bir bağlam içerisinde sunulmasıdır. Son olarak manipülasyon ise seçme, ekleme veya çıkarma yoluyla değiştirilmiş bilgiye karşılık gelmektedir (Fallis, 2014b: 142).

Yakın tarihte öne çıkan ve dezenformasyonlara sahne olmuş siyasal olayları sıralamak da meseleyi bütüncül bir açıdan ele alma yolunda önemlidir. Bunlar 2011 yılında zirveye ulaşan Arap Baharı, 2013 yılında Türkiye’de Gezi Olayları, Mısır’da Cumhurbaşkanı Mursi’nin devrilmesi ve Brezilya’da başlayan sokak olayları neticesinde Devlet Başkanı Dilma Rouseff’in iktidardan uzaklaştırılması olarak sıralanabilmektedir. Kamuoyunda tartışılan ve dezenformasyonu barındıran diğer hadiseler ise ABD 2016 Başkanlık Seçimleri’ne Rusya’nın müdahalesi iddiası, Türkiye’nin 2018’de Zeytin Dalı Harekatı sırasında karşılaştığı dezenformasyon kampanyası ve 2020’de Azerbaycan ve Ermenistan arasındaki çatışmalar sırasında sosyal medya kanalları üzerinden yürütülen dezenformasyon operasyonlarıdır.

### **3. Dezenformasyonla Mücadelede Üç Farklı Aktör: NATO Stratejik İletişim Mükemmeliyet Merkezi, Anadolu Ajansı, Teyit.org Örnekleri**

Dezenformasyonla mücadele yanıtlanması gereken bir diğer soru ise tehdide karşı kimin önleyici veya koruyucu olacağı sorusudur. Yukarıda da bahsedildiği gibi dezenformasyonun ve günümüzün güvenlik paradigmasındaki konumunun çok boyutlu dinamiği ona karşı mücadelenin de çok boyutlu, diğer bir ifadeyle hibrit olmasını gerektirmektedir. Çalışmanın bu bölümünde dezenformasyon tehdidiyle mücadele noktasında birbirinden farklı üç kurum ve faaliyetleri açıklanacaktır. Bu kurumlardan NATO Stratejik İletişim Mükemmeliyet Merkezi uluslararası düzlemde faaliyet gösteren bir güvenlik kurumu olma mahiyetine sahiptir. Bir diğer kurum olan Anadolu Ajansı ise bir doğruluk kontrolü kurumu olmamasına rağmen Türkiye’nin 2018 yılında Zeytin Dalı Harekatı sırasında karşılaştığı dezenformasyon kampanyasına karşı bir süreliğine doğruluk kontrolü yayınları yapmıştır. Anadolu Ajansı devlete bağlı bir haber ajansı olmakla birlikte dezenformasyonla mücadeleye katılması bir anlam ifade etmektedir. Son olarak bir sivil toplum aktörü olan teyit.org tamamıyla doğruluk kontrolü üzerine kurulmuş ve çalışmalarına devam eden bir aktördür.

#### **3.1.NATO Stratejik İletişim Mükemmeliyet Merkezi**

NATO Stratejik İletişim Mükemmeliyet Merkezi (StratCom), Letonya’nın başkenti Riga’da 2014 yılında kurulmuş uluslararası düzeyde bir güvenlik kurumu olarak konumlandırılmaktadır. Varlık sebebini “savaşların insanların zihninde başladığı ve savunmanın da zihinde başlaması gerektiği” anlayışı üzerinde kurgulanmaktadır. StratCom, NATO’nun yedi üye devleti Estonya, Almanya, İtalya, Letonya, Litvanya, Polonya ve Birleşik Krallık tarafından imzalanan bir mutabakat zaptıyla çalışmalarına başlamıştır. 1 Eylül 2014 tarihinde NATO akreditasyonunu alan kurum NATO’nun çabalarına stratejik iletişim açısından bir katkı sağlamak amacıyla kurgulanmıştır.

StratCom’un kurumsal yapısı NATO’nun komuta yapısının bir parçası olmamakla birlikte, kurum NATO adına bir açıklama yapma ehliyetine sahip değildir. NATO’nun gelişmekte olan rolleri, hedefleri ve misyonları hakkında uygun, zamanında, doğru ve duyarlı bir şekilde iletişim kurmasını incelemektedir. Merkezin misyonu, NATO, NATO müttefikleri ve NATO ortaklarının stratejik iletişim yeteneklerine somut bir katkı sağlamak üzerine şekillenmiştir. StratCom, sivil ve askeri, özel ve akademik sektörlerden çok uluslu ve sektörler arası katılımcılar tarafından oluşturulan ve modern teknolojiler, analiz, araştırma ve karar verme için sanal araçları kullanan bir nitelikte kurgulanmıştır. Merkezde çeşitli alanlardan sivil ve askeri uzmanlar, eğitmenler, analistler ve araştırmacılar çalışmaktadır.

Esasen StratCom dezenformasyonla mücadeleden daha geniş bir tanımla çalışmaktadır. Ancak Merkez’in yayınlarına bakıldığında son dönemde dezenformasyonla mücadele üzerine eğildiği görülmektedir. Bu durum dezenformasyon tehdidinin ne denli ciddi bir tehdit haline geldiğinin de göstergesi olarak değerlendirilebilmektedir.

Merkez, sponsorluk yapan ülkeler ve katkıda bulunan katılımcılar tarafından yönetildiği ve finanse edildiği belirtilmektedir. Başlangıçta Letonya, Estonya, Almanya, İtalya, Litvanya, Polonya ve Birleşik Krallık tarafından kurulan bu yapıya 2016’da Hollanda ve Finlandiya, 2017’de İsveç, 2018’de Kanada ve 2019’un başlarında Slovakya, 2020’de Danimarka ve Amerika Birleşik Devletleri, 2021’de Macaristan, 2024’te ise İspanya Merkez’e katılmıştır. Fransa ve Avustralya, Merkez’e katılım süreçlerini başlatmıştır (StratCom.com, 2025).



StratCom'un 2024 yılında gerçekleştirdiği faaliyetlere bakıldığında şu başlıklar göze çarpmaktadır (StratCom.com, 2025):

- NATO StratCom ve MilPA doktrin yönetimi
- Yıllık StratCom TTX konsept geliştirme ve Bilgi Ortamı Simülasyon Alanı
- “Ukrayna’daki askeri eylemleri desteklemek ve hedef kitleleri etkilemek için Rusya’nın İletişim Stratejisi” çalışması
- “Batı bilgi ortamı dışındaki Rus bilgi operasyonları (Asya, Afrika, Latin Amerika)” çalışması
- Ukrayna StratCom ortaklık programı
- Akdeniz bölgesindeki göç kriziyle ilgili hedef kitle algısı
- İklim ve çevre temelli kötü niyetli bilgi etkisi faaliyetleri üzerine çalışma
- Arktik’teki anlatılar ve kötü niyetli bilgi operasyonları
- Platform düzenlemesinin dezenformasyon bağlantısı üzerindeki etkisinin değerlendirilmesi
- Bilgi doğrulama ve geçerlilikte Yapay Zekanın (Generative AI) etkisini ve gelecekteki rolünü analiz etme
- Bilgi Ortamı Değerlendirme kursları
- “İletişimciler için yapay zeka araçları” kursu
- Sosyal Medya Manipülasyonu deneyi
- NATO ve ulusal tatbikatlara destek
- NATO StratCom eğitim ve öğretim desteği
- NATO StratCom ve IEA El Kitabı

### 3.2. Anadolu Ajansı’nın Doğruluk Kontrolü Çalışmaları

Anadolu Ajansı (AA) 1920 yılında kurulan bir devlet haber ajansıdır. AA, yıllarca haber havuzu oluşturma ve resmi etkinliklerin duyurulması görevlerini ifa ettikten sonra, 2010’lu yıllarla birlikte bir vizyon değişikliğine gitmiştir. Bu vizyon değişikliğiyle birlikte AA, çalışma kapsamını geliştirmiş ve genişletmiş, bünyesindeki yabancı dil birimlerini artırmış ve daha geniş bir spektrumda haber yayıncılığına başlamıştır. Ajans haber yayıncılığının dışında çeşitli uluslararası gelişmelere dair analiz ve görüş yazılarını yayınlamayı da görev edinmiştir. 2020 yılından itibaren AA, bünyesinde bir araştırma masası kurulmasıyla birlikte yalnızca metin olarak değil video üretimleriyle de çeşitli araştırma dosyalarını kamuoyuna sunmaya başlamıştır (Anadolu Ajansı, n.d.).

2018 yılının Ocak ayında Türk Silahlı Kuvvetleri tarafından başlatılan ve Suriye’nin kuzeyindeki Afrin bölgesinde konuşlanmış PKK/YPG militanlarının tasfiye edilmesini amaçlayan Zeytin Dalı Harekatı sürecinde, Türkiye çeşitli dezenformasyon girişimlerinin hedefinde yer almıştır. Çok farklı merkezler tarafından yürütülen ve Türk askerinin hareket meşruiyetine zarar vermeyi amaçlayan bu dezenformasyon kampanyası sürecinde AA, bir doğruluk kontrolü faaliyetine başlamıştır. Esasen yakın zamana kadar doğruluk kontrolü gibi bir görevi olmayan AA, bir devlet ajansı olarak hibrit bir tehditle karşılaştığı bilinciyle bu faaliyetlere başlamıştır. Bu durum, bu çalışmada da vurgulanan dezenformasyonun doğasının ve onunla mücadele yöntemlerinin hibrit ve çok boyutlu olduğu tezini doğrulamıştır.

Terör örgütü PKK/YPG bu süreçte gerçeklikle ilgisi olmayan görseller ve metinlerle dezenformasyon kampanyasının merkezinde yer almıştır. AA ise doğruluk kontrolü prensibiyle bu görsellerin esasen hangi olay ve bağlama ait olduğunu bildirmiş ve bunu kamuoyuna yayınlamıştır. Bu süreçte AA, sosyal medya kanallarını etkili bir şekilde kullanmıştır. AA, bahsi geçen süreçte 13 dilde yayın yapmıştır. Bu doğruluk kampanyasının temelinde “Afrin Afrinlileridir.” mesajı yer almış, ayrıca Zeytin Dalı Harekatı’nın temel hedefinin siviller değil terör unsurları olduğu sıklıkla vurgulanmıştır (Toktay, 2019).

AA, 2022 yılında dezenformasyonla mücadele adına yeni bir adım atmış, bünyesinde bir teyit editörlüğü kurmuştur (Yeni Şafak, 2022). Ajans, Teyit Hattı olarak isimlendirilen bu yapıyı tanıtımında, tüm dünyada yürütülen araştırmaların haber kaynaklarının çeşitlendiğini gösterdiğini, küresel düzeyde tüketim alışkanlıklarının internet ve sosyal medyaya taşındığını vurgulamaktadır. Yine Ajans'a göre İnternet platformlarının Türkiye'de de en çok başvurulan içerik kaynağı haline gelmesi yanıltıcı içerik miktarında da artışa sebep olmuştur. Bu nedenle gazeteciliği kamu görevi olarak tanımlayan Ajans, yanıltıcı içerikle mücadelede sorumluluk üstlenmek üzere Teyit Hattı'nı kurmuştur. Teyit Hattı'nın faaliyet alanı kamuoyunun doğru bilgi edinmesini önlemek üzere dolaşıma sokulan her içeriği kapsamaktadır. Ajansın bu görev üzerine kurduğu ekip, gerek metin gerekse görsel tüm yanıltıcı içerik ve haberlerin orijinal biçimlerinin kamuoyuyla paylaşılması üzerine çalışmaktadır. Ajans, bilgi kirliliği ve dezenformasyonun çok boyutlu doğasını kabul etmekte ve bunlarla mücadelede yeni biçim ve yöntemlere başvurma güdüsüne sahip olduğunu vurgulamaktadır. Ajans, son olarak son yüzyıldaki gazetecilik tecrübesine güvendiğini belirtmekte, bu tecrübesi ve tüm dünyadaki muhabir ağının gücünü doğruluk kontrolüyle bütünleştireceğini ifade etmektedir (Anadolu Ajansı, 2022).

### 3.3. Teyit.org

Teyit.org 2016 tarihinde kurulan, internet temelli bir doğruluk kontrolü kuruluşudur. İnternet sitesi üzerinden faaliyetlerini sürdüren bu girişim, kendisini yaygın bilinen yanlışları, sosyal medyada yer alan şüpheli bilgileri, medyada yer alan yanlış iddiaları araştırmak ve raporlamak olarak kurgulanmıştır. Teyit.org'un temel çalışma alanı internet ortamı olmakla birlikte, birincil haber kaynağı olarak interneti kullanan kişilerin ve sivil toplum kuruluşlarının doğru bilgileri teyit etmeleri, yanlış bilgilerden ise olumsuz şekilde etkilenmemeleri yönünde bir çalışma yürütülmektedir. Teyit.org aynı zamanda yeni medya okuryazarlığını artırmayı ve eleştirel düşünme alışkanlığını kazandırmayı amaçladığını bildirmektedir (teyit.org, 2020).

Teyit.org internet üzerinden haber taraması yapmakta, doğruluğundan şüphe duyulan haberleri inceleme sürecine almakta ve analiz sonuçlarını kullanıcılarıyla paylaşmaktadır. Teyit.org'un doğrulama süreci tarama, seçme ve önceliklendirme, araştırma ve yayınlama olarak aşamalandırılmaktadır. Tarama aşamasında şüpheli haberler taranmakta ve platformun yönetim panelinde toplanmaktadır. Seçim ve önceliklendirme aşamasında paneldeki haberler doğrulanabilirlik, yaygınlık ve önem kriterlerine göre önceliklendirilmektedir. Araştırma ve yayınlama aşamasında ise yanıltıcı içerik iddiaları platform editörleri tarafından araştırılmakta ve analiz edilmektedir. Son olarak ilgili haberin doğru, yanlış veya doğruluğu belirsiz olması gibi bir değerlendirme yapılmakta ve yayına sunulmaktadır (Karadağ ve Ayten, 2020: 492).

Teyit.org'un kurumsal yapısı ise kâr amacı gütmeyen bir sosyal girişim olarak konumlanmıştır. Kuruluş açıkça bir sivil toplum aktörüdür ve NATO StratCom ve AA'dan farklı şekilde esnek bir insan kaynağına sahiptir. Kurumun gelir kaynağı ise kitle fonlamasından ABD Büyükelçiliği'ne, Heinrich Böll Vakfı'ndan Facebook'a kadar çeşitlilik göstermektedir (Ünver, 2020: 5).

Platform internet sitesinde oldukça geniş kapsamdaki faaliyetlerini tanıtmaktadır. Atölyeler kapsamında teyitçilik, dijital okur yazarlık, dijital güvenlik eğitimlerinin bulunduğu vurgulanmaktadır. Teyit.org bu eğitimlerinde herkesin bir teyitçi gibi eleştirel düşünme becerilerini geliştirebilmesi için çaba gösterdiğini ifade etmektedir. Platform Pürmerak Kulübü isimli çevrimiçi eğitim platformuyla dijital okur yazarlık becerileri geliştirmeyi amaçlamaktadır. Dijital Veli isimli e-bülten, platformun velilere özel hazırladığı, ebeveynlerin dijital okur yazarlık becerilerini güçlendirmeyi amaçlayan yayın organıdır. Bu e-bültenle yalnızca velilerin değil, onlar üzerinden çocukların da bilginin doğruluğu üzerine bilinçlerinin geliştirilmesi hedeflenmektedir. T cetveli isimli podcast serisi ise platformun bilgi, medya, internet ve sosyal medyaya dair konuları incelediği sesli yayın organıdır (Teyit.org, 2024).

Kuruluş son yıllarda "Fact(ory)" adında bir girişim başlatmış, bu girişimle bir iş geliştirme sürecine girmiştir. Bu girişimle yanlış bilgi ve haber sorununa yenilikçi ve sürdürülebilir çözümler geliştirilmesi hedeflenmiştir (Çalıköğlü, 2023).

## Sonuç

Dezenformasyon kampanyaları günümüz dünyasında öne çıkan tehditlerden birisi olarak kabul edilmektedir. Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, özelde de kitle iletişim teknolojilerinin çok kaynaklı bilgi paylaşımına müsaade eden yükselişi bireyler ve toplumların haber alma ve psikolojik sağlıklarına yönelik dezenformasyon girişimlerini kolaylaştırmıştır. Çok boyutlu bir tehdit olarak kabul edilebilecek dezenformasyon, onunla mücadelenin de çok boyutlu ve çok aktörlü olmasını gerektirmektedir.

Yaşanan bu dönüşüm ve öne çıkan tehditlerin çeşitlenmesi, güvenlik yaklaşımlarında bir değişimi de beraberinde getirmiş, yeni güvenlik yaklaşımları güvenliğin referans nesnesine birey ve toplumu yerleştirmiştir. İletişimin ve haberleşme hakkının güvenliği ancak merkeze meta yerine insanı konumlandırarak kavranabilmektedir. Dezenformasyonun iletişim ve güvenlik sisteminde konumlandırılması da bireyin haklarının korunması ilkesiyle sağlanabilmektedir.

Dezenformasyonla mücadeledeki çok boyutlu ve çok aktörlü yaklaşım ihtiyacını vurgulamak üzere kurgulanmış bu çalışmada bir uluslararası güvenlik kuruluşu olan NATO'ya akredite Stratejik İletişim Mükemmeliyet Merkezi, son yıllarda dezenformasyon kampanyalarına ciddi ölçüde maruz kalmış bir devletin haber ajansı olan Anadolu Ajansı ve sivil toplum girişimi olarak doğruluk kontrolü yapmak üzere konumlanan teyit.org yapıları incelenmiştir. Birbirinden farklı yapı ve motivasyonlara sahip bu üç kurum da doğruluk kontrolü faaliyetleriyle yanlış bilgilerin kamuoyunda yayılmasına engel olmaya çalışmaktadır.

NATO StratCom, dezenformasyonla mücadelede uluslararası düzeyde önemli bir aktör olarak öne çıkmaktadır. Özellikle Ukrayna krizindeki bilgi operasyonlarına yönelik çalışmaları, NATO müttefikleri arasında stratejik iletişim alanında bir kapasite inşasına katkı sağlamıştır. StratCom'un ürettiği raporlar ve düzenlediği simülasyonlar, NATO üyesi ülkelerin kamuoylarını yanlış bilgilendirme girişimlerine karşı daha dirençli hale getirmeyi amaçlamaktadır. Ancak, StratCom'un uluslararası bir kurum olması, doğrudan bireysel kamuoyları etkileme kapasitesini sınırlayabilmektedir. Stratejik hedeflerine ulaşma açısından değerlendirilirse, kurumun özellikle müttefik devletler arasında stratejik iletişim kapasitesini güçlendirmede başarılı olduğu, ancak bireysel halk katmanlarına erişimde daha geniş ölçekli projelere ihtiyaç duyduğu ifade edilmelidir.

Anadolu Ajansı, dezenformasyonla mücadelede özellikle Zeytin Dalı Harekâtı sırasında gerçekleştirdiği doğruluk kontrolü faaliyetleriyle dikkat çekmiştir. Bu dönemde, görsel materyallerin doğrulanması ve harekâtın hedeflerine ilişkin net mesajların yayılması, kamuoyunun dezenformasyona karşı direnç geliştirmesine katkıda bulunmuştur. Ajansın devlet destekli bir yapıya sahip olması, doğruluk kontrolü çalışmaları sırasında operasyonel kapasitesini artırmıştır. Ajansın kurumsal kimliği doğruluk kontrolünde yetkinlik açısından kendisine bir güç sağlamıştır.

Teyit.org, dezenformasyonla mücadelede uzmanlaşmış bir doğruluk kontrolü platformu olarak faaliyet göstermektedir. Çalışmalarında şeffaf ve sistematik bir metodoloji kullanması, platformun doğruluk kontrolü süreçlerinin güvenilirliğini artırmaktadır. Özellikle eğitim programları ve dijital okuryazarlık projeleri, bireylerin yanlış bilgiye karşı farkındalığını artırmayı hedeflemektedir. Bununla birlikte, Teyit.org'un etki alanı daha çok bireysel düzeyde bilgi tüketicileriyle sınırlıdır. Kamu kurumları veya büyük medya kuruluşları üzerinde daha geniş bir etki yaratabilmek için daha kapsamlı işbirliklerine ve stratejik projelere ihtiyaç duyduğu görülmektedir.

21. yüzyılın ikinci on yılında güvenlik konseptini güncelleyen ve yeni bir bakış açısıyla güvenlik sorunlarına yaklaşan Türkiye'nin "yeni güvenlik konsepti", üzerine daha fazla akademik literatür geliştirilmesi gereken bir kavramdır. Türkiye bölgesel ve küresel düzeydeki riskleri sınır ötesinde karşılama, dış politika ve yumuşak güç kurumlarıyla güvenliğe proaktif yaklaşma faaliyetlerinin yanında halkın haber alma hakkının ve psikolojik sağlığının güvenliğini de dikkate almak durumundadır. Cumhurbaşkanlığı yapısı altında kurulan İletişim Başkanlığı, Dijital Dönüşüm Ofisi ve Siber Güvenlik Başkanlığı, Türkiye Büyük Millet Meclisi bünyesinde kurulan Dijital

Mecralar Komisyonu, Emniyet Genel Müdürlüğü ve diğer güvenlik kurumlarının siber güvenlik birimleri iletişim ve güvenlik kavramlarının kesiştiği noktada faaliyete başlamışlardır. Yeni güvenlik konseptini bütüncül bir şekilde uygulamaya devam etmek, bu kurumların stratejik iletişim yaklaşımıyla koordine edilerek dezenformasyonla mücadeleyi öncelikledikleri müddetçe mümkün olacaktır.

### Kaynakça

- Allcott, H., ve Gentzkow, M., (2017), Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), 211-36.
- Anadolu Ajansı (2022). *Teyit hattı hakkında*. Erişim adresi: <https://www.aa.com.tr/tr/teyithatti/p/teyit-hatti-hakkinda->
- Anadolu Ajansı (n.d.). *Tarihçe*. Erişim adresi: <https://www.aa.com.tr/tr/p/tarihce>
- Arcos, R., Gértrudix, M., Arribas, C., & Cardarilli, M. (2022). Responses to digital disinformation as part of hybrid threats: a systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking. *Open Research Europe*, 2. <https://doi.org/10.12688/openreseurope.14088.1>.
- Arquilla, J. ve Ronfeldt, D. (1996). The Advent of Netwar. *RAND Corporation*.
- Arslan A. C., (2023). *Intelligence Analysis: Reproduction of Information*, Ankara: Polis Akademisi Yayınları.
- Ayhan, U. (2016). Yeni Güvenlik Konsepti ve Güvenliği Sınır Ötesinde Karşılama. *Turkish Journal of Security Studies*, 18(3), 133-142.
- Ağır, B. S. (2015). Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı. *Güvenlik Stratejileri Dergisi*, 11(22), 97-130.
- BBC.com, (2016), 'Post-truth' declared word of the year by Oxford Dictionaries. (2016, November 16). E.T.: 12 Aralık 2020, <https://www.bbc.com/news/uk-37995600>
- Boghardt, T. (2009). Soviet Bloc intelligence and its AIDS disinformation campaign. *Studies in Intelligence*, 53(4), 1-24.
- Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Cangızbay, K. (2000). *Hiçkimsenin cumhuriyeti*. Ütopya Yayınevi.
- Çalıkoglu, B. (2023). *Yeni medya ekosisteminde bir topluluk deneyimi: factory*. Erişim adresi: <https://teyit.org/ekipten/yeni-medya-ekosisteminde-bir-topluluk-deneyimi-factory>
- Dedemen, F., (2016), Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi. *Güvenlik Bilimleri Dergisi*, 5(1), 141-176.
- Fallis, D. (2014a). A functional analysis of disinformation. *iConference 2014 Proceedings*.
- Fallis, D. (2014b). The varieties of disinformation. İçinde *The philosophy of information quality* (pp. 135-161). Springer, Cham.
- Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1), 4586.
- Hama, H. (2017). State Security, Societal Security, and Human Security. *Jadavpur Journal of International Relations*, 21, 1 - 19. <https://doi.org/10.1177/0973598417706591>.
- Hammond-Errey, M., ve Ray, K. (2019). A new methodology for strategic assessment of transnational threats. *Police Practice and Research*, 22, 40 - 56. <https://doi.org/10.1080/15614263.2019.1699411>.
- Karadağ, G. H. ve Ayten, A. (2020). A comparative study of verification/fact-checking organizations in Turkey: dogrulukpayi. com and teyit. org. *Motif Akademi Halkbilimi Dergisi*, 13(29), 483-501.
- Mumford, A. (2020). Understanding hybrid warfare. *Cambridge Review of International Affairs*, 33, 824 - 827. <https://doi.org/10.1080/09557571.2020.1837737>.
- Newman, E. (2001). Human Security and Constructivism. *International Studies Perspectives*, 2, 239-251. <https://doi.org/10.1111/1528-3577.00055>.
- StratCom. (2025), About Us. *StratCom*, [www.stratcomcoe.org/about-us](http://www.stratcomcoe.org/about-us).
- Teyit.org. (2020), *Şüpheli bilgileri inceleyen doğrulama platformu*, [teyit.org/nedir](http://teyit.org/nedir).

- Teyit.org. (2024). *Eğitim*. Erişim adresi: <https://teyit.org/egitim>
- Toktay, Y. (2019). *Sosyal medyada dezenformasyon, manipülasyon ve propaganda etkisi: zeytin dalı hareketi örneği*. Yayınlanmamış Yüksek Lisans Tezi.
- Urhal, Ö. (2009). *Küreselleşen dünyada güvenlik: milli güvenlik, kamu güvenliği, örgütlü suçlar ve suç istihbaratı*. Adalet Yayınevi.
- Ünver, H. A., (2020). *Türkiye’de doğruluk kontrolü ve doğrulama kuruluşları*. EDAM.
- Waltz, K. (1979). *Theory of international politics*, McGraw.
- Yayla, A. (2020). Totaliterizm ve dezenformasyon. *Liberal Düşünce Dergisi*, 25(98), 125-146.
- Yeni Şafak (2022). *Anadolu Ajansı teyit editörlüğü kurdu*. Erişim adresi: <https://www.yenisafak.com/hayat/anadolu-ajansi-teyit-editorlugu-kuruldu-3858109>

### **Çatışma beyanı**

Makalenin yazarı, bu çalışma ile ilgili taraf olabilecek herhangi bir kişi ya da finansal kuruluş ile ilişkisi bulunmadığını dolayısıyla herhangi bir çıkar çatışmasının olmadığını beyan eder.

### **Destek ve teşekkür**

Çalışmada herhangi bir kurum ya da kuruluştan destek alınmamıştır.