Yönetim Bilimleri Dergisi/Journal of Administrative Sciences
Cilt/Volume: 22, Sayı/No: 53, ss./pp.: 1205-1230
DOI: https://doi.org/10.35408/comuybd.1457165

-ARAŞTIRMA MAKALESİ-

RUS DIŞ POLİTİKASINDA SİBER MÜDAHALE YÖNTEMİ OLARAK DEZENFORMASYON OPERASYONLARI*

Yücel BAŞTAN[1] & Filiz ÇOBAN ORAN[2]

Öz

Devletlerin siber uzayı dış politika amaçlarına ulaşmak için kullanmaları, siber uzayın devletler ve uluslararası örgütlerce bir rekabet alanı olarak benimsenmesine neden olmuştur. Bu nedenle devletler siber uzayın güvenliğini, bir güvenlik sorunu olarak algılamakta ve dış politikalarında bir araç olarak kullanmaktadır. Siber uzayda gerçekleştirilen çeşitli müdahale yöntemlerinden biri hedef ekosistemde bilgi operasyonlarının yürütülmesidir. Bilgi operasyonu yöntemlerinden biri olan dezenformasyon, bilgi savaşlarında kullanılan stratejilerden biridir. Dezenformasyon devletlerin hem barış hem de çatışma dönemlerinde kamuoyunu kasten yanlış yönlendirmek, manipüle etmek için kullandıkları bir yöntem olduğu için Uluslararası İlişkiler literatüründe çalışılmaya başlanmıştır. Bu bağlamda bu çalışma, dezenformasyon olgusunu bir dış müdahale aracı olarak tanımlamaktadır. Literatüre göre, Rusya hibrit savaş taktiklerinden biri olarak dezenformasyon operasyonunu en çok uygulayan ülkelerden biridir. Bunun için bu çalışma Rusya'nın 2016 ABD başkanlık seçimlerinde yürüttüğü siber müdahale örneğine odaklanarak, bir dış müdahale aracı olarak dezenformasyon taktiklerini nasıl uyguladığını açığa çıkarmayı amaçlamaktadır. Çalışmada, kavramsal ve yöntemsel çerçeve çizildikten sonra Rusya dış politikasında dezenformasyonun yeri tarihsel olarak ele alınmaktadır. Örnek olay analizi sonucunda, 2016 ABD Başkanlık seçimlerinde Rusya'nın Sovyetler Birliği döneminde kullandığı "beyaz, gri ve siyah faaliyetler" şeklinde gruplanan propaganda yöntemlerini kullandığı iddia edilmektedir. Böylelikle ulusal seçim dönemlerinde bilgi ekosisteminin güvenliğinin önemine dikkat çeken bu çalışma, Rus dış politikasında dezenformasyon taktiklerinin nasıl kullanıldığının daha iyi anlaşılmasına katkıda bulunmaktadır.

Anahtar Kelimeler: *Siber Müdahale, Dezenformasyon, Rus Dış Politikası, ABD Seçimleri, Siber Güvenlik.*

Jel Kodları: *H56, F52.*

Başvuru: *22.03.2024* **Kabul:** *01.07.2024*

---

* Bu çalışma, ÇOMÜ LEE Uluslararası İlişkiler Anabilim Dalı Doktora Programı'nda Yücel Baştan tarafından hazırlanan "Dış Politika Aracı
Olarak Dezenformasyon: Rusya'nın Türkiye'ye S-400 Satım Sürecinde Sputnik Haber Kanalı Tweetlerinin İncelenmesi" adlı doktora tez
çalışmasından üretilmiştir

[1] Arş. Gör. Dr., Çanakkale Onsekiz Mart Üniversitesi Siyasal Bilgiler Fakültesi Uluslararası İlişkiler Bölümü, yucel.bastan@gmail.com, Çanakkale, Türkiye, ORCID: 0000-0002-6808-6790.
[2] Doç. Dr., Çanakkale Onsekiz Mart Üniversitesi Biga İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, filizcoban@comu.edu.tr, Çanakkale,Türkiye, ORCID: 0000-0003-1789-8411.

DISINFORMATION OPERATIONS AS A METHOD OF CYBER INTERVENTION IN RUSSIAN FOREIGN POLICY[3]

Abstract

The use of cyberspace by states to achieve their foreign policy objectives has led states and international organizations to adopt cyberspace as an area of rivalry. Thus, states perceive cyberspace security as a security issue and instrumentalize it in their foreign policy. One of the various intervention methods used in cyberspace is to carry out information operations in the targeted ecosystem. Disinformation is one of the information operation methods that is used as an effective strategy in information wars. Since disinformation is a method used by states to deliberately mislead and manipulate public opinion both in times of peace and conflict, it has been studied in the International Relations literature. In this context, this paper defines the phenomenon of disinformation as a means of foreign intervention. According to the literature, Russia is one of the countries that most frequently uses disinformation operations as a hybrid warfare tactic. Therefore, this study aims to reveal how Russia has used disinformation tactics as a form of foreign intervention, focusing on its cyber interference in the 2016 US presidential elections. After outlining the conceptual and methodological framework, the study examines the historical place of disinformation in Russian foreign policy. As a result of the case study analysis, it claims that Russia used Soviet propaganda methods grouped as "white, grey, and black activities" during the 2016 US Presidential elections. Highlighting the importance of the security of the information ecosystem during national election periods, this study contributes to a better understanding of how disinformation tactics are used in Russian foreign policy.

Keywords: *Cyber Intervention, Disinformation, Russian Foreign Policy, USA Elections, Cyber Security.*

JEL Codes: *H56, F52.*

"Bu çalışma Araştırma ve Yayın Etiğine uygun olarak hazırlanmıştır."

1. GİRİŞ

İletişim ve internet teknolojilerinin yaygınlaşması, devletlerin dış politika amaçlarını gerçekleştirmek için giriştikleri rekabet alanını genişletmiş, devletler yeni rekabet alanlarını yeni yöntemlerle kullanmaya başlamıştır (Bıçakçı, 2019). Kullanılan yeni alanlardan/yöntemlerden bazıları hibrit savaş kapsamında değerlendirilmektedir. Hibrit savaş;siyasi hedeflere ulaşmak için aynı anda konvansiyonel ve konvansiyonel olmayan güçlerin, değişken taktiklerde kullanımı olarak tanımlanmaktadır (Wither, 2016; Hoffman, 2014; Mansoor, 2012). Hibrit savaş sırasında farklı araç ve yöntemlerin kullanılması ulusal güvenlik için, kapsam ve yoğunluk açısından değişkenlik gösteren tehditler oluşturmaktadır (Bağbaşlıoğlu, 2021, s.8). Hibrit tehdidi kullanmak isteyen devletler, organizasyon yeteneklerine odaklanarak asimetrik avantaj elde etmeye çalışmaktadır. Elde edilecek asimetrik avantaj sadece askeri üstünlük değildir; enformatik, ekonomik, mali ve yaptırım hukukunu barındıran

[3] The Extended English Summary is located the end of the Article

ulusal gücün tüm unsurlarıyla bütünsel bir üstünlüktür (McCulloh ve Johnson, 2013: 2-3). Savaş sahası dışında asimetrik avantaj elde etmek isteyen devletler çeşitli yöntemler kullanmaktadır. İnternet ve sosyal medyanın oluşturduğu bilgi ekosistemine yapılan müdahalelerde bu kapsamda değerlendirilmektedir. Bu makale, bir hibrit tehdit ve siber müdahale yöntemi olarak dezenformasyon uygulamasını dış politika aracı olarak değerlendirmekte kullanılan yöntemlerin siyasi niteliğini Rusya örneği bağlamında araştırmaktadır.

Literatürde Rusya'nın siber saldırılarına ilişkin hatırı sayılır sayıda çalışma bulunmaktadır (Willett, 2022; Kostyuk ve Brantly, 2022; McCrory, 2020; Zhao vd, 2023; Jensen, vd., 2019). Bununla birlikte bir siber müdahale yöntemi olarak "dezenformasyon operasyonlarına" ilişkin sınırlı sayıda çalışma bulunmaktadır (Erlich ve Garner, 2023). Oysaki siyasi sonuçları dikkate alındığında ve Rusya'nın siber alanda uyguladığı dezenformasyon stratejilerinin sonuçları incelendiğinde, siber alanın taktik seviyede etkin şekilde kullanıldığı görülmektedir (Ellehuus, 2020). Bu durum ise Rusya'nın dezenformasyon operasyonlarını dış politikasında bir müdahale yöntemi olarak kullandığını göstermektedir. Rusya'nın bilgi operasyonları üzerine çalışmalar yapmak, Rusya'nın dış politika amaçlarına ulaşmak için dezenformasyon yöntemlerini sıklıkla tercih etmesinden ötürü daha çok akademik ilgiyi hak etmektedir. Örneğin, Rusya'nın 2014 yılındaki Ukrayna müdahalesinde kullandığı tekniklerin, konvansiyonel ve konvansiyonel olmayan operasyonların kombinasyonunu içerdiği bilinmektedir (Laruelle ve Limonier, 2021). Yine Rusya'nın Kırım'ı ilhakı ve Doğu Ukrayna'daki ayrılıkçı gruplara verdiği destek sırasında kullandığı araçlar konvansiyonel muharebenin yanında; siyasi protestoları, ekonomik zorlamaları, siber operasyonları ve özellikle dezenformasyon kampanyalarını da içermektedir. Eski NATO Genel Sekreteri Anders Fogh Rasmussen, bu eylemleri hibrit savaş olarak tanımlarken, Rusya'nın askeri operasyonlarının saldırgan dezenformasyon kampanyalarını da kapsadığını belirtmiştir (Lander ve Gordon, 2014). 2014 yılında Kırım ile ilgili kampanyanın merkezinde yer alan bilgi savaşları taktik düzeyde elektronik ve siber savaş üzerinden ilerleyerek Ukrayna'nın cevap verme yeteneğini etkisiz hale getirmiştir. Yalan ile gerçek arasında oluşturulmak istenen bulanıklıkta başarılı olunmuş ve olaylar Rus medyasının bakış açısıyla sunulmuştur (Wither, 2016). Benzer biçimde Rusya, 2022 yılında Ukrayna'yı işgalinde askeri güç kullanımının yanı sıra siber alandaki faaliyetlerini dış müdahale aracı olarak kullanmıştır.

Bu çalışma, Rusya'nın özellikle seçim dönemlerinde Batı demokrasilerine karşı aktif olarak uyguladığı, literatürde "siber seçmen müdahalesi" (Hansen ve Lim, 2019) ya da "etki operasyonu" (Larson vd., 2009) kavramlarıyla da anılan dezenformasyon operasyonlarıyla ilgilenmektedir. Beklenmedik şekilde Donald Trump'ın seçimi kazanıp başkanlık koltuğuna oturduğu, 2016 ABD seçimlerine yönelik yapılan çalışmalar (Pope 2018; McCombi vd., 2020), Rusya'nın siber müdahale uygulayarak seçim sonucunu etkilediğini göstermektedir. Bu çalışma bu örneğe odaklanarak, Rusya'nın bir siber müdahale yöntemi olarak uyguladığı "dezenformasyon" faaliyetlerini incelemeyi amaçlamaktadır. Diğer çalışmalardan farklı olarak bu çalışma, Rusya'nın uyguladığı dezenformasyon stratejisinin kaynağını ortaya koyarak

ve yöntemlerini sınıflandırarak 2016 ABD seçimlerindeki siber müdahalesinin daha iyi anlaşılmasını sağlamaktadır. Böylelikle Rusya'nın seçim döneminde bilgi operasyonlarını tek boyutlu değil, çok boyutlu ve organize şekilde gerçekleştirdiğini göstermektedir. Bu amaçla çalışma, Rusya Federasyonu'nun dezenformasyon stratejilerinin Sovyetler Birliği propaganda ve dezenformasyon stratejilerine benzerliğini açığa çıkarmakta, Sovyet döneminde beyaz, gri ve siyah olarak tanımlanan propaganda/dezenformasyon: faaliyetlerinin ABD seçimlerinde siyasi hedeflerini gerçekleştirmek için taktik seviyede kullanıldığını ortaya koymaktadır. Çalışmada Rusya'nın uyguladığı stratejinin açığa çıkarılması, diğer ülkeler uyguladığı veya uygulayacağı dezenformasyon stratejisinde kullanacağı yöntemlerin daha iyi anlaşılmasını sağlayacaktır.

Bu çerçevede çalışmada, öncelikle Uluslararası İlişkiler literatüründe siber müdahale ve dezenformasyon kavramının yerine açıklık getirilecektir. Ardından Rusya'nın Sovyetler Birliği'nden günümüze bilgi operasyonları ve dezenformasyon stratejileri tarihsel olarak ele alınarak, Rus dış politikasında dezenformasyonun hangi yöntemlerle uygulandığı araştırılacaktır. Örnek olay analizinde (Yin, 2003), 2016 yılındaki ABD başkanlık seçimleri incelenerek, Sovyetler Birliği döneminde "beyaz, gri ve siyah propaganda/dezenformasyon faaliyetleri" olarak tanımlanan dezenformasyon yöntemlerini günümüzde Rusya'nın ABD seçimlerinde nasıl uyguladığı gösterilecektir. Böylelikle çalışmada, Rusya'nın yürüttüğü/yürüteceği dezenformasyon stratejilerinin boyutları açığa çıkarılıp çözümlenerek Rusya'nın dezenformasyon stratejisinin daha iyi anlaşılması sağlanmaktadır.

2. ULUSLARARASI İLİŞKİLERDE REKABET ALANI OLARAK SİBER ALAN

İnternet, Soğuk Savaş döneminde devletlerarası rekabet sonucu bulunmuştur. 1957 yılında Sovyet Rusya'nın ABD'den önce dünya yörüngesine Sputnik uydusunu fırlatması ABD'nin nükleer tehdit algısının boyutunu değiştirmiştir. SSCB'nin uyduyu fırlatması ile ABD topraklarının saldırıya uğrayabileceğini düşünerek nükleer saldırıya karşı ikinci vuruş yeteneğini kaybetmemek için savunma bakanlığı AR-GE çalışmalarına önemli bir bütçe ayırmıştır. Bunun sonucunda İleri Araştırma Projeleri Ajansı (Advanced Research Project Agency, ARPA) bilinen ve daha sonra adı İleri Savunma Araştırma Projeleri Ajansı (Defence Advanced Research Project Agency, DARPA) olarak değiştirilen kurum günümüzde internet olarak hizmet veren etkileşimli bir bilgisayar kompleksini geliştirmiştir. Yaklaşık on yıl içinde birkaç düzine bilgisayarı birbirine bağlayan ağlardan oluşan ARPANET geliştirilerek bugün kullandığımız anlamda internete dönüştürülmüştür.

Soğuk Savaş sonrası dönemde Sovyet tehdidinin ortadan kalkmasıyla internetin açık ve özgür olması fikri yayılmış, devletler, sermaye ve bireylerin internetin özgür şekilde kullanmaları ve interneti şekillendirebilmelerinin önünü açmıştır. İnternetin küresel alanda geliştirilmesi ve yaygınlaştırılması için altyapı sistemlerine (fiber optik kablo ağlar, bilgisayarlar, yazılımlar v.s.) ihtiyaç duyulmuştur. Sermayenin bu ihtiyacı görmesi ve ABD'nin girişimcileri bu alana yönlendirmesiyle yeni bir ekonomi

doğmaya başlamıştır. ABD, neo-liberal dış politika anlayışıyla uyumlu biçimde internet üzerinde geniş düzenlemelerden kaçınarak sermaye eliyle internet ekonomisinin oluşmasına destek vermiştir. Ayrıca, müdahaleci düzenlemelere karşı çıkarken, dijital bilgiyi herkesçe erişebilir hale getirmeye çalışmıştır (Mansell 2012). Bunda teknolojinin özgürleştirici gücüne olan inançla dış politikada demokrasilerin teşvik edilmesi anlatısı önemli rol oynamıştır. Teknolojik ilerlemeye eşlik eden sermaye (start-uplar ve Silikon Vadisi) küresel özgürlük mücadelesine dahil edilmeye çalışılmıştır (Morozov, 2012; Shirky, 2011).

ABD'nin anlatısına karşı demokratik olmayan devletler bu alanı vatandaşlarını gözlem altında tutmak için kullanmaya başlamıştır. Böylelikle özgürlük demokrasi, bilgi güvenliği gibi anlatılara karşı anlatılarla cevap verilmiştir (Starr, 2019). Yani otoriter rejimlerin kendi anlatıları ile demokrasi anlatısına yetiştiğini ifade etmek mümkündür (Cohen ve Fontain, 2020). Örneğin Çin internet teknolojilerini kendi kamuoyuna yönelik daha yoğun olarak kullanırken, Rusya iç ve yakın dış kamuoyuna yönelik devlet anlatısını hâkim kılmak üzere interneti aktif şekilde kullanmaktadır. Google yerine Yandex, Facebook'a karşı V Kontakte gibi uygulamalarla Rusça konuşan ülkeler üzerinde daha yoğun faaliyet göstermektedir. Çin ise, ABD anlatısının kendi ülkesinde etkili olmasına izin vermemektedir. WhatsApp gibi anlık mesajlaşma uygulamalarının yanında Facebook, Instagram, Twitter, Pinterest ve Reddit gibi birçok sosyal medya ağı Çin'de yasaklanmıştır (French, 2021). Çin, bu uygulamaların alternatiflerini çıkartarak kendi vatandaşlarının kullanımına açmıştır. Çin'de en yaygın kullanılan Qzone yanında; Twitter benzeri bir uygulama olan Weibo, WhatsApp benzeri bir uygulama olan WeiXin ve MySpace benzeri bir uygulama olan Douban gibi birçok sosyal medya uygulaması bulunmaktadır (Savitz, 2012). Çinliler, Qzone adlı uygulamaya yüklenen sanal paraları gerçek hayatta kullanabilmekte böylece sanal para üzerinden alışveriş yapabilmektedirler (Goh, 2009). Böylesi büyük bir veri ile yapay zekâ destekli farklı algoritmalar kullanılarak kullanıcıların şahsi birçok özelliğini ortaya çıkarmak mümkündür. Çinli firmanın sahip olduğu TikTok dünya genelinde en çok kullanılan uygulamalardan biri olmasının yanında Batılı ülkelerin özellikle veri güvenliği sebebiyle şüphelerini ve endişelerini ilettiği bir uygulamadır (Hirsch vd., 2022; Pollina, 2022). Kısacası, internet devletlerin kendi iç ve dış politika yaklaşımlarını yansıttıkları politik bir rekabet alanı olarak yıllardır farklı şekillerde kullanılmaktadır.

Genel anlamda insanların bilişim sistemleriyle birbirine bağlı olduğu etkileştiği ve birbirine bağlı bilişim sistemlerinin birbirleri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alan "siber uzay" olarak tanımlanmaktadır (Bıçakçı, 2014). Bu çerçevede siber uzayı genişleten en önemli etmenin internet olduğu ifade edilebilir. "Siber alan" kavramlaştırması ise NATO gibi güvenlik örgütleri ile devletlerin siber uzayı; kara, deniz, hava, uzay gibi bir alan olarak tanımlanmasını ifade etmektedir. Bu çerçevede siber alan aynı zamanda içinde; siber espiyonaj, siber savaş, siber güvenlik, yapay zekâ gibi birçok kavramı barındıran ve devletlerin mücadele ettiği bir mücadele alanını ifade etmektedir. Bu mücadele alanına yönelik devletlerin ve uluslararası örgütlerin ilgisinin artması ve literatürde üzerine yapılan

tartışmaların yoğunlaşmasında temel olarak üç olay etkili olmuştur: Estonya siber saldırısı, Arap Ayaklanmaları, 2016 yılında Rusya'nın ABD seçimlerine müdahalesi. Estonya siber saldırıları: 2000 yılında başkent Tallinn'de "Tallinn'in Kurtarıcısı" (Bronz Asker) heykelinin yıkılmasını isteyenler ve yer değiştirilmesini isteyenler arasındaki tartışmanın ardından heykelin Tallinn askeri mezarlığına taşınması sonucu siyasi bir gerginlik meydana gelmiştir. Bunun ardından Estonya'da yaşayan Rus kökenli vatandaşların gösterileri ile eş zamanlı ülkenin siber altyapısını hedef alan siber saldırılar gerçekleştirilmiştir. Bu saldırılar, banka altyapıları ile başbakanlık, parlamento ve bakanlıkların siteleri, siyasi partilerin siteleri ve medya kurulları ile iletişim firmalarına dönük olarak gerçekleştirilmiştir. Bu saldırılar 28 Nisan'da zirveye ulaşmış ve 9 Mayıs tarihinde İkinci Dünya Savaşı'nda Rusya'nın Almanya'yı yendiği gün, bot net saldırılarına dönüşmüştür (Bıçakçı 2012). Günlük hayatı uzun süre etkileyen saldırılara NATO'nun karşılık verememesinin nedenlerinin başında, bu saldırıların silahlı çatışma hukuku çerçevesinde değerlendirilmemesi ve daha önce planlanmamış bir saldırı biçimine yönelik yeterli savunma/saldırı aksiyonunun verilememesidir. Bunun yanında saldırıların Rusya tarafından yapıldığı kabul edilse de saldırıları üstlenen veya kabul eden devlet bulunmamaktadır (Schmitt 2017).

Estonya saldırılarının ardından 2004 yılında Estonya'nın NATO'ya önerdiği Siber Savunma Mükemmeliyet Merkezi'nin (Cooperative Cyber Defence Centre of Excellence) kurulma süreci hız kazanmıştır ve merkez Tallinn'de kurulmuştur. Merkezin çalışmaları arasında siber alanda ortak yeteneğin geliştirilmesi ve üye devletlerden birine saldırı durumunda diğer devletlerin ortak hareket etme kabiliyetinin geliştirilmesidir. Böylelikle NATO'nun siber caydırıcılığına katkıda bulunmaktadır. Merkezin önemli çalışmaları arasında Schmitt editörlüğünde hazırlanan Tallinn El Kitabı (Schmitt, 2013, 2017) bulunmaktadır. Kitabın amacı, siber savaşlarda uygulanması gereken uluslararası hukuk kurallarına (jus in bello) yönelik kapsamlı bir altyapı hazırlanmasıdır. Kitap, genel olarak siber savaşa girmenin haklı nedenlerinin (jus ad bellum) yanı sıra siber savaş sırasında takip edilecek kuralların çerçevesini çizmeyi amaçlarken siber uzayı bir alan olarak tanımlamakta ve her devletin kendi egemenlik alanında hak sahibi olduğunu iddia edilmektedir (Çelik, 2013). Bu açıdan, siber alanda devletlere egemenlik hakkı tanınması siber müdahaleler bağlamında uluslararası hukuktaki "saldırı suçu" tanımlamasını da genişletmektedir.

Arap Ayaklanmaları: 2011 yılının bahar aylarında Ortadoğu ve Kuzey Afrika ülkelerini etkisi altına alan Arap ayaklanmaları sırasında halk sosyal medyadan örgütlenmiş ve haberleşmiştir. Böylelikle sosyal medyada yayılan bilgilerin önemli sonuçlar doğurabileceği ortaya çıkmıştır. Bilgi yayma ve gündem oluşturma konusunda medya; hükümet ve kamuoyu arasında son derece kilit bir role sahiptir (Çoban 2016). Halk ayaklanmalarında sosyal medyanın etkili kullanımı, internetin uluslararası ilişkiler gündeminde daha sık yer almasına neden olmuştur (Tremayne 2014). Geleneksel medyada bulunan eşik bekçilerinin sosyal medyada bulunmaması bilgi hiyerarşisini yıkmıştır. Bilgi ve kullanıcılar arasındaki ilişkide yıkılan hiyerarşi bilgi örgütlenmesindeki süreçlerin yeniden ele alınmasına neden olmuştur. Tabandan örgütlenen yeni ağ modelinde sosyal medya aynı zamanda siyasi hareketlerin

koordinasyonu içinde önemli araç haline gelmiştir. İster baskıcı olsun ister demokratik olsun tüm aktörler ülkedeki rejimi etkilemek için internete bağlı platformları kullanmaktadır.

Tabandaki hareketlerin Arap ayaklanmaları sırasında üst seviyede değişimlere sebep olması sosyal medya üzerinden devlet anlatılarının yayılması ve sosyal medya ekosisteminde devletlerin yer alması gerektiği algısını güçlendirmiştir. Demokratik devletlerde ise uygulanan politikalarda mümkünse tabanın rızasının oluşturulması, mümkün değilse tabandan büyük bir itirazın gelmemesi önemlidir. Bu sebeple tabanı etkileyecek ve rıza oluşturacak anlatılar devletler ve devlet dışı aktörler tarafından önemsenmektedir. Sosyal medyanın oluşturduğu bilgi ekosisteminde bilgi savaşlarının temel sebebi, her aktörün tabanın mümkünse rızasını maksimuma çıkarma, mümkün değilse de itirazları en aza indirme çabasıdır. Bu sebeple internet erişimi olan herkesin ücretsiz kullanım hakkına sahip olduğu sosyal medya, platformları başta devletler olmak üzere aktörlerin anlatılarının tabanı etkilemek üzere çarpıştığı yeni bir alan olma özelliğine sahiptir. Demokrasilere yönelik dezenformasyon faaliyetlerinin özellikle seçim zamanlarında (Bentzen,2019) artmasının sebebi budur.

Birbirini tanımayan farklı coğrafyalardan birçok insanın etkileşimde olduğu sosyal medya platformları internetin doğasından gelen özgür ve erişilebilir olarak tasarlanmıştır. Öte yandan, sosyal medya mimarisini basit şekilde platformlara işlerlik kazandıran tasarım olarak görmemek gerekir. Sadece etkileşimle sohbet etme etkileşimde bulunma gibi eylemlerin ötesinde bunlar, toplumun yaşam şekillerini analiz eden, nasıl organize edilebileceğini içinde barındıran özelliklere sahiptir (Parker vd. 2016). Elde ettikleri verilerle beslenmekte ve algoritmalar ve arayüzler bu veriler ışığında şekillenmektedir. Daha da önemlisi, insanların çoğunlukla verilerini rızaya dayalı paylaşmalarıdır. Unutulmamalıdır ki, sosyal medya platformuna sahip şirketin amacı kar elde etmektir. Bunun için daha çok kullanıcı aktif olarak platformda bulunmalıdır. Böylelikle kullanıcılardan elde edilen veriler pazarlanarak daha çok kar elde edilebilmektedir. Daha çok kullanıcının bulunduğu sosyal medya bu sebeple dezenformasyonun yayılabilmesi için önemli avantaj sağlamaktadır.

2016 Yılındaki ABD Başkanlık Seçimleri: 2016 yılında ABD'de Hillary Clinton ve Donald Trump arasında geçen başkanlık seçimi yarışında Rusya'nın Cumhuriyetçi aday Donald Trump'ın seçilmesi için siber müdahalede bulunduğu bilinmektedir. Bu dış müdahaleyi diğerlerinden ayıran üç temel özellik bulunmaktadır. Birincisi, müdahalede konvansiyonel yöntemlerin kullanılmamasıdır. İkincisi, siber alanın sunduğu fırsatlar aracılığı ile Rusya, coğrafi olarak uzak olan ve farklı dil kullanan bir ülke olan ABD'ye karşı rahatlıkla konvansiyonel olmayan yöntemler kullanılabilmiştir. Üçüncüsü, başkanlık seçimi gibi karar vericilerin belirlendiği kritik bir süreçte bilgi operasyonlarının kullanılmasıdır. Dolayısıyla bu çalışma, Rusya'nın dezenformasyon uygulama taktik ve stratejilerini daha iyi anlamak için bu örneğe odaklanmaktadır.

3.ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ: SİBER MÜDAHALE

Devletler dış politika amaçlarına ulaşabilmek için çeşitli yöntemler kullanmaktadır. Bu yöntemlerden ilk akıllara gelen sınıflandırma diplomatik, askeri ve ekonomik araçlar olarak ifade edilebilir. Bu sınıflandırma devletlerin stratejik hedeflerine ulaşmak için uyguladığı politikaların genel çerçevesini vermese de taktik seviyede farklı müdahalelerin yapıldığı bilinmelidir. Müdahale kavramının çerçevesi oldukça geniştir. Rosenau (1968), müdahale ilgili genel çerçeve çizerken iki durumdan hareket etmek gerektiğini ifade etmektedir. İlk olarak müdahale geleneği bozan bir harekettir ve bir otorite tarafından yönlendirilmelidir. İkinci olarak ise müdahale sınırlı ve geçici olmalıdır. Genel çerçevesini çizerken müdahaleyi uluslararası ilişkilerde alışıldık olmayan, yani geleneksel olmayan durumlar olarak tanımlamaktadır. Müdahale ne kadar uzun sürer ve devamlılık arz ederse geleneksel hale geleceği için, kavram araştırılırken sonu olan geçici eylemler üzerinde durulmalıdır. Bir diğer çalışmasında Rosenau (1969) kavram ile ilgili yapılan eylemin yapılmama durumunda hedefteki grubun eylemlerinde değişiklik olmayacağını ifade etmektedir.

Plant (1993) müdahale kavramını, devletlerin iç politikasını etkilemek için eylem ve eylemsizlik olarak tanımlamaktadır. Herhangi bir eylemlerin müdahale olarak değerlendirilebileceğini ifade ederken, eylemsizliklerin de müdahale olarak kabul edilebileceğini belirtmiştir. Örneğin, Afganistan ve Pakistan'dan Türkiye'ye gelen düzensiz göçmenlere yönelik İran tarafının eylemde bulunmaması Türkiye'nin güvenliğine yönelik bir müdahale olarak kabul edilebilir.

Siber müdahale kavramını incelerken üç temel zorlukla karşılaşılmaktadır. Siber müdahale kavramına yönelik yaygın bir literatür bulunmaması ve uluslararası hukukta siber müdahale kavramına yönelik bir tanımlamanın bulunmaması, karşılaşılan ilk zorluktur. Uluslararası hukuk normu bulunmamasına rağmen, NATO Siber Savunma Mükemmeliyet Merkezi tarafından Schmitt editörlüğünde uzmanlar grubu tarafından hazırlanan ve siber savaşlarda uyulması gereken uluslararası hukuk kuralları (jus in bello) ve siber savaşa girmenin haklı nedenleri (jus ad bellum) kitapta açıklanmaktadır. Siber uzayı alan olarak tanımlayan kitap, her devletin siber uzayda egemenlik hakkı olduğunu iddia etmekte ve bir devletin diğer devletin iç ve dış işlerine siber araçlarla zorlayıcı müdahalede bulunamayacağını ifade etmektedir.
Siber müdahale kavramının incelenmesindeki diğer sorun, siber alanda gerçekleştirilen müdahalenin hangi aktör tarafından gerçekleştirildiğinin çoğunlukla net şekilde belirlenememesidir. Bir devlete karşı siber alanda gerçekleştirilen müdahalenin aktörleri çoğunlukla belirlenememektedir. Örneğin, 2010 yılında İran'ın nükleer santrallerine yapılan Stuxnet saldırılarını kimin düzenlediği henüz belirlenememiştir.

Siber müdahale kavramı üzerine çalışırken karşılaşılan üçüncü sorun ise hangi eylemlerin müdahale kapsamında değerlendirileceği sorunudur. Medya aracılığıyla sürekli yapılan bilgi düzensizlikleri geleneksel bir durum aldıysa, bunun müdahale kapsamında değerlendirilip değerlendirilmeyeceği tartışmalı bir konudur. Özellikle seçim dönemleri gibi ülke siyasetinde son derece etkili değişiklik yapma potansiyeli

olan zamanlarda taktik seviyede yapılan bilgi alanına müdahaleler, siber müdahale kapsamında değerlendirilmelidir. Bu taktik adımlar çoğunlukla, troller ve bot saldırıları ile müdahalenin etkisini artırıcı eylemleri de kapsamaktadır. Ayrıca sınırlı ve süreli olan siber saldırıları da siber müdahale çerçevesinde değerlendirmek mümkündür. Bu çerçevede oltalama ve fidye yazılımlar gibi kar elde etme amaçlı siber saldırıları devlete yönelik müdahale kapsamında değerlendirilemezken, Stuxnet, Estonya saldırıları, 2008 yılında Gürcistan'a gerçekleştirilen siber saldırılar (Gerdia-Ruddia Conflict, cyberlaw, 2022) arkasında siyasi bir motivasyon olması sebebiyle siber müdahale kapsamında değerlendirilebilir.

3.1. Siber Müdahale Türü Olarak Dezenformasyon

Türk Dil Kurumu, bilgi kavramını "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü; bili, malumat" şeklinde tanımlamaktadır. Felsefi anlamına, "duyu organları yoluyla algılama, hayal gücü ve bellek yardımıyla zihnin ilk olarak kavradığı temel düşünceler" olarak yer verirken, bilişimdeki anlamına "verinin anlam kazanmış biçimi" tanımlamasıyla açıklama getirmektedir (sozluk.gov.tr,2024). Bu genel tanımlamalardan hareketle bilgi kavramı ile insanların günlük rutinleri arasındaki bağlantıyı kurmak mümkündür. Yeni elde edilen bilgi üzerinden düşünülecek olursa, bir şeyin insan zihninde bir olgu oluşturması anlamına gelmektedir. Bu olgu ise genel bilgilerin gerçekliğinin sabit olmasının yanında bilgiyi veren aktör tarafından şekillendirilebilmektedir, yani bilgi yeniden üretilebilmektedir. Bu çerçeveden bakıldığında günlük hayatta karşılaştığımız birçok kişi ve durumun yanı sıra televizyon, radyo ve internet aracılığıyla edindiğimiz bilgiler dünya hakkında görüşlerimizi şekillendirmektedir. İletişimin matematiksel teorisini oluşturmak isteyen Shannon (1948), iletişim döngüsünün 5 öğe barındırdığını ifade etmektedir: bilgi kaynağı, verici, gürültü kaynağı, alıcı ve hedef.

Şekil 1: Shannon'un İletişim Döngüsü

Bu döngüdeki sorun, ilk mesajın tam veya yaklaşık olarak son noktada yeniden üretilmesidir. Geleneksel medya üzerinden düşünülecek olursa, bir karar verici ile yapılan röportaja farklı bir yorum eklenerek geleneksel medya kanalları aracılığı ile kişi nihai hedefe yönlendirilebilir. Geleneksel medya bu sebeple halka hangi bilgilerin ulaştırılacağı, bu bilgilerin hangi önem derecesi ile ifade edileceği gibi kriterleri belirleyebilmektedir. Otoriter rejimlerde medya, yöneticinin tekelinde aynı zamanda bilgiyi elinde tutabilme ve halkı istediği şekilde yönlendirebilme yeteneğine sahipken demokratik rejimlerde medya yönetime eleştirel de bakabilir. Yasama, yürütme ve yargının ardından liberal toplumlarda dördüncü güç olarak kabul edilen medya kamusal çıkarı savunmak adına yönetici söylemini halka eleştirel şekilde iletebilmektedir. Bunun yanında medyanın kapital doğası siyasal yapı ile bütünleşik davranabilmesine neden olabilmektedir (Erdoğan, 2013). Medyanın siyasal iktidarla

yakın ilişkileri ve temelde kamu yararını savunması beklenmesine rağmen sermaye olarak kurulan doğası sebebiyle sorgulanmaktadır. Yönetimlerle tartışılmaz maddi-manevi ilişkisi olan medya kuruluşları paylaşacakları haberlerde meşrulaştırıcı bir dil, üslup, içerik veya fotoğraf kullanıp kullanmayacakları ile ilgili yönetimlerle pazarlık edebilmektedir (Denk, 2007:152).

Dolayısıyla, tüm bilgilerin bir arada bulunduğu bilgi ekosisteminde medya kanalları önemli güç unsuru olmaktadır. Nihai olarak medyanın iletişim döngüsündeki bilgi kaynağı ile hedef arasında etkili olduğu ve farklı meydana gelen bir olayı (bilgi) farklı şekillerde verebildiğini ifade etmek mümkündür. Bu yönüyle medya hedef kitleye ulaşmak isteyen hükümetler, devletler veya karar vericiler için araç olabilmektedir. Bu sebepledir ki devlet anlatısını kendi ülkesinde ve diğer ülkelerde hakim/etkili kılmak isteyen ülkeler kendi medya kanallarının diğer halkların dillerinde de yayın yapmalarını sağlayarak, uluslararası topluma mesajlarını yaymaya çalışmaktadır.
Aktörler bilgiyi kontrol ederek hedefteki kişinin görüşlerini kendi anlatıları doğrultusunda şekillendirmek isterler. Dezenformasyon ile amaçlanan da budur. Sovyetler birliğinin uyguladığı; beyaz, gri ve siyah propaganda/dezenformasyonun amacı da nihai olarak budur. Kendi anlatısının yayılması öncelikli olmasa bile karşı devlet anlatısının bozulması ve hedef kitlenin belirli kararlara yönlendirilmesi amacıyla kullanılan dezenformasyonun en etkili örneği 2016 ABD seçimleri sırasında gerçekleştirilmiştir.

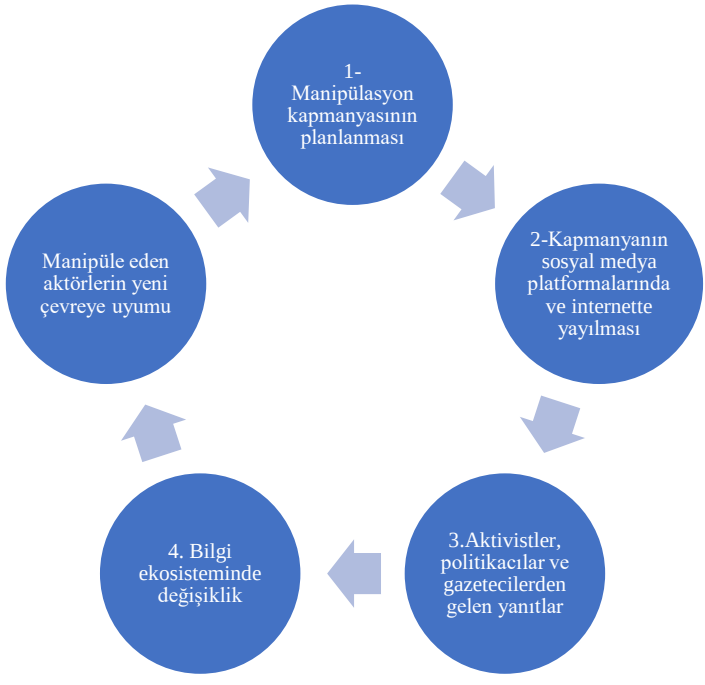
Bilgi düzensizliği yöntemlerinden olan dezenformasyon kişi, grup, kuruluş veya ülkeye zarar vermek amacıyla oluşturulan yanlış bilgiler olarak ifade edilmektedir. Dezenformasyon taktik ve stratejik seviyelerde kullanılabilmektedir (Brantly, 2020:27). Gri alanda kalan bir yöntem olarak tanımlanan dezenformasyon (Hicks ve Friend, 2019), propaganda kavramına benzerlikleri sebebiyle karıştırılabilmektedir. Hem propaganda hem dezenformasyon siyasi hedeflere ulaşmak için kasıtlı olarak manipülatif bilgilerin yayılmasını içermektedir. Propaganda siyasi hedefe ulaşmak için kitlenin görüşlerini şekillendirmek olarak tanımlanırken, dezenformasyon yanlış veya yanıltıcı bilginin kasten yayılmasıdır. Bu anlamda propagandanın çok daha geniş bir kapsama sahip olduğunu ifade etmek mümkündür (Benkler, 2018).
Daha açıklayıcı olmak gerekirse, dezenformasyonun üç özelliği olduğu ifade edilebilir (Fallis, 2015). İlk olarak dezenformasyon anlamsal içeriği olan bilgidir. İkinci özellik bu bilginin yanlış inançlar yaratması muhtemel olan yanıltıcı bilgi olmasıdır. Son olarak, bu bilgi tesadüfi değildir; yani dezenformasyon içeren bilgi kasıtlı olarak hazırlanmıştır.

Siber müdahale yöntemi olarak dezenformasyon, taktik niyetle bilgi ortamını değiştirmeyi veya kirletmeyi amaçlamaktadır. Nihai olarak karar verme sırasında karar verici aktörlerin görüşlerini değiştirmeye veya alınacak kararlarda şüphe duyulmasına yani bilgi sisi yaratılması amaçlanmaktadır. Böylelikle karar verici berrak olan suyu bulandırarak alınacak kararda ihtiyatlı tartışmalara ve tarafsız bilgilerin analizine yol açarak karar verme süreçlerinde sistemin hızlı ve etkin işlemesinin önüne geçmeye çalışmaktadır. Bilgi ekosisteminde bilgi düzensizliğinin yaratılması, önemli konularla ilgili fikir birliğine varan karar vericilerin gerçek

hakkında fikir birliğine vardığı durumlarda dahi medyada yer alan haberler ve haberler dışındaki raporlardan elde edilen bilgilerin manipüle edilmiş olabileceği algısı yaratılır (Whyte ve Manazec, 2018: 235). Libicki'nin deyimiyle (2007) dezenformasyon aslında bilginin dolaylı olarak yok edilmesidir. Karar vericinin karar verme aşamasındaki bilgiye eklenen dezenformatif bilgiler ile bilgi güvenliği bozulur. Bilginin değiştirilmesi yani gürültü eklenmesi ile taşınan bilgi bozulmuş olur. Nihai olarak alınan karar etkilenmiş en azından alınan kararların doğruluğundan şüphe duyulması sağlanır veya karara yeterince güvenmeleri engellenir.

Dezenformasyonun neden yapıldığı sorusunun tek motivasyonu siyasi değildir. Siyasi motivasyonun yanında tık almak veya reklamlardan para kazanmak gibi maddi motivasyonlar veya sosyal/psikolojik motivasyonlarda bulunabilir (Wardle, 2020:12-13). Dolayısıyla devletler, para kazanmak motivasyonu ile hareket eden sermaye veya bireyler de dezenformasyon gerçekleştirebilir. Bu yöntemler ise "müdahale" kapsamında değerlendirilmemelidir.

Harvard Üniversitesi'nin Medya, Politika ve Kamu Politikası Shorenstein Merkezi'nin teknoloji ve sosyal değişim araştırma ekibi (2020) "medya manipülasyonunu", kamuoyunun dikkatini çekmek ve aldatıcı, yaratıcı veya adil olmayan yollarla kamu söylemini etkilemek için bilgi ekosistemindeki belirli koşullardan/özelliklerden yararlandıkları süreç olarak tanımlamaktadır. Medya manipülasyonu kavramını ise dezenformasyon, bilgi operasyonları veya etkileme operasyonları gibi çeşitli terimlerin yer aldığı geniş çatı bir terim olarak kullanmaktadır. Buna göre medya manipülasyonu yaşam döngüsü aşağıdaki gibidir(Harvard Kennedy School, 2020):



Şekilde de görüleceği üzere özellikle sosyal medyadan yapılan dezenformasyon sadece yaygın kitleye ulaşabilmesi sebebiyle değil aynı zamanda niteliği sebebiyle de önemlidir. Twitter üzerinden örneklendirilirse, bir kişinin dünya görüşünün ve beğenilerinin analizi tüm etkileşimler üzerinden yapılmaktadır. Ardından kişinin twittter da bulunma süresinin artırılması böylelikle kişi hakkında daha fazla bilgi edinilmesi ve bu bilginin pazarlanabilmesi için kişiler kendi görüşlerinden insanların bulunduğu yankı odalarında bulunmaktadır. Yani genellikle kendi görüşlerinden olan kişilerin paylaşımlarını daha sık görmektedir. Dolayısıyla dezenformasyon içeren bilgi sisteme en etkili olacak grup üzerinden girmektedir. Ardından bu dezenformatif bilgi çeşitli araçlarla internet ve sosyal medyada yaygınlaştırılmaktadır. Daha sonra bu bilgiye gelen tepkiler üzerinden dezenformasyona uğramış bilgi yeniden üretilerek sisteme tekrar girdi olarak sunulmakta veya o bilgiyi destekleyecek yeni bilgilerle bilgi ekosisteminde dezenformasyona sahip bilgi etkin kılınmaktadır. Sosyal medya, bilginin yaygınlaşmasını sağlamasının yanında kişilerin analizlerinin çıkarılabilmesi ve gelen tepkilerin ölçülebilmesi sebebiyle dezenformasyon yapılabilmesi için etkin olarak kullanılabilmektedir.

4. RUS DIŞ POLİTİKASINDA DEZENFORMASYONUN YERİ: RUSYA'NIN BEYAZ, GRİ VE SİYAH YÖNTEMLERİ

Bu çalışma Rusya'nın günümüzde kullandığı dezenformasyon stratejisinin kaynağı Sovyetler Birliği döneminde kullanılan yöntemlere dayandığını iddia etmektedir. Bununla birlikte günümüzde kullanılan yöntemler sosyal medya üzerinden

yaygınlaştırılmaktadır (Isachenkov,2017). 1917 yılında Bolşevik devrimi ile SSCB'nin kuruluşunun ilk yıllarında bilgi kontrolü ve bilgi manipülasyonu konuları ön planda yer almıştır. Kuruluşunda Sovyetler Birliği'nin ilk öncelikli güvenlik kaygısı dış saldırılardan ziyade içeride yönetimini güçlendirmektir. Bu sebeple ülke içinde bilgi kontrolünün sağlanması ve yeni yöntemlerin geliştirilmesi gerekli görülmüştür (Brantly, 2020:27). Rusya'nın iç ve dış politikada silahlı kuvvetler ve cumhuriyetin müdafaası amacıyla Artuzov tarafından 1923 yılında kurulan ve Unshlikht tarafından devam ettirilen dezenformasyon ofisi kurulmuştur. Kurum Kuruşçev tarafından KGB'de A direktörlüğünün kurulmasıyla zirve noktasına ulaşmıştır. A direktörlüğü ordu hakkında İngilizlere, Fransızlara, Japonlara ve Almanlar gibi çeşitli ülkelerin silahlı kuvvetlerine kendi ülkeleri hakkında yanlış bilgiler vererek Kızıl Ordu'ya olduğunun üzerinde yetenek atfedilmesine neden olmuştur. Sovyet yeteneklerinin %95'inin Rusya'nın dezenformasyonu sonucu elde edilmesi (Haslam, 2015:31) dezenformasyonu başarılı şekilde kullanıldığını göstermektedir.

Sovyetlerin genel olarak hibrit güç yeteneği geliştirmesinde Hitler Almanya'sının önemli etkisinin olduğunu ifade etmek mümkündür. Almanya'dan hissedilen varoluşsal tehdit ve Almanya'nın konvansiyonel yeteneği SSCB'nin hayatta kalması için hibrit güç yeteneğini geliştirmesine ve etkili şekilde kullanmasına neden olmuştur. Almanya karşısında geri çekilen Kızıl ordunun geride bıraktığı alanlarda Sovyet partizanların mücadele için hibrit yöntemler geliştirmiştir. Bu yöntemler askeri teknolojilerin yanında askeri olmayan, terörist, diğer suç unsurlarının kullanımını da içeren geniş çerçeveli konvansiyonel olmayan yetenekleri de içermektedir. Sovyet partizanlar için geliştirilen yöntemler, hibrit savaşın doğasında olan asimetrik avantajı zaman zaman sağlayabilmiştir. Hibrit yöntemlerle sağlanan avantaj Kızıl Ordu'nun 1944 yılında geniş çaplı saldırısına zemin hazırlamıştır (McCulloh ve Honsson, 2013: 2-3). Nihayetinde SSCB'nin savaş sırasındaki propagandaları kaybedilen yerlerin kazanılmasına katkı sağlamıştır (Thompson,1991).

1959 yılında kurulan ve D bölümü olarak adlandırılan dezenformasyon birimi doğrudan Komünist Parti Prezidyumu'na bağlı hareket etmiştir. 1962 yılında ise Kuruşçev'in ABD üstünlüğünü aşındırmak için D departmanını KGB'nin birinci baş müdürlüğünde özel birimden biri olan ve A1 olarak da bilinen daha büyük organizasyona yükseltilmiştir. Kuruluşundan 5 yıl sonra birimin var olduğu gerçeği öğrenilmiştir. ABD istihbarat raporlarına göre yılda 350-400 operasyon yürüten birim, Igor Agayants'ın ofisin başına geçmesiyle daha etkin şekilde kullanılmaya başlamıştır. Agayants'a göre dezenformasyon görevlileri, yaratıcılık, kültürel empati ve alışılmışın dışında düşünme gibi yeteneklere sahip olmalıdır ayrıca çalışmalarında titiz ve disiplinli olmalıdır. Böylelikle Agayants önderliğinde dezenformasyon birimi kariyer yapma alanı haline gelmiştir. Birim, düşmanların başarısızlıkları ve kırılganlıklarının belirlenmesi ve analiz edilmesiyle dünya genelinde sistematik olarak yapılan analizleri kullanarak güvenlik açıklarından faydalanmıştır (Rid, 2020: 167-168).

SSCB'de dezenformasyon çalışmaları beyaz, siyah ve gri olmak üzere üçe ayrılmaktadır. Beyaz propaganda/dezenformasyon, Moskova radyosu, Tass ve Novostinews ajansları ile büyükelçilikler tarafından açık faaliyetler şeklinde yapılmaktadır. Siyah propaganda ise daha örtülü olarak gerçekleştirilmektedir. KGB ajanları tarafından sahte haberlerin yayılması, yalan ve utanç verici hikayelerin oluşturulması ve yerleştirilmesi siyah propaganda faaliyeti çerçevesinde değerlendirilmektedir. Gri propaganda ise NATO füzelerinin Batı Avrupa'ya yerleştirilmesine karşı gösteri yapan Dünya Barış Konseyi ve Dünya Sendikalar Federasyonu gibi çeşitli grupları içermektedir. Bu çerçevede bilim insanları, doktorlar, gazeteciler ve öğrencilerle yapılan faaliyetler ve verilen destekler gri faaliyet alanı çerçevesinde değerlendirilmektedir(Snyder,2012:24-25).Beyaz propagandayı/dezenformasyonu resmi araçlarla ifade edilen dezenformasyon veya yönlendirme içeren bilgiler, siyah propaganda/dezenformasyon, örtülü gerçekleştirilen ve doğrudan devletin gerçekleştirdiğine yönelik bilgi bulunması kolay olmayan daha saldırgan bilgiler ve gri propaganda/dezenformasyon ise devletin desteklediği, örgütlediği veya bir şekilde bağlantısının bulunduğu 3. aktörler tarafından yapılan propaganda/dezenformasyon faaliyetleri şeklinde gruplandırmak mümkündür.

SSCB'nin son döneminde propaganda ve dezenformasyon faaliyetleri politikasında değişiklikler yaşanmıştır. 1980'lerin ortalarında Gorbaçov'un politika değişikliği ile Batı'ya karşı bakışın değişmesi ve Batı ile iş birliği yollarının arandığı dönemdir. Günümüzde Rusya'nın propaganda ve dezenformasyona yönelik şaşırtma ve propaganda yapanın çıkarları doğrultusunda hareket ettiğinin farkına varmadan hedefleri elde edilmesinin sağlanması Soğuk Savaş teknikleri üzerine kuruludur. Yani Rusya, Sovyetler Birliği dönemindeki tecrübelerinde dayanarak günümüz bilgi sisteminde etkili olmaktadır (Paul ve Matthews, 2016). Sovyetler Birliği elindeki medya organları, Komünist Parti'nin mesajlarını iletmek ve devletin tarafından belirlenen yönlendirmeleri vatandaşın takip etmesini sağlamak üzerine yayınlar yapmıştır. Mevcut Rus medya sisteminin kendine has özellikleri olmasına rağmen Sovyetlerden gelen bazı unsurları, otosansür gibi, kullandığı tespit edilebilmiştir (Potter, 2019).

Rusya'nın günümüzdeki politikalarını, SSCB sonrası Batı ile birlikte hareket edilmesi gerekenlerin savunanların güçsüzleştiği dönem ile başlatmak mümkündür. 1992-1998 yıllarında liberal düşünenlerin hakimiyeti Batı ile iyi ilişkiler kurarak Rusya'nın gelişmiş ülkeler arasında yer alması gerektiği görüşü çerçevesinde şekillenmiştir. Yeltsin'in kendi kaderini tayin hakkı politikası sonrası oluşan iç karışıklıklar ve ekonomik sorunlar döneminde Rusya'nın ABD hegemonyasını kabul ettiği yıllar olarak adlandırmak mümkündür. Rusya'da bu politikaların değişmesi gerektiğini savunan Yevgeni Primakov, 1996-1998 yılları arasında Rusya Dışişleri Bakanlığı, 1998-1999 yıllarında ise Rusya Başbakanı olarak görev yapmıştır. Primakov tarafından uygulanan dış politika, Rusya'nın realizme dönüşünü de temsil etmektedir (Hamzaoğlu,2020).

Primakov tek kutuplu dünya düzeni fikrinin tarihsel gerçeklerle bağdaşmadığını, bunun Soğuk Savaş'ın ardından Batı'nın Doğu'yu bozguna uğrattığı görüşüne dayandığını ifade etmektedir. Bununla birlikte Primakov'a göre Doğu bozguna uğramamıştır. Sovyetlerin tasfiyesi çelişkiler ve Ukrayna ve Beyaz Rusya'nın subjektif kararları sonucu içsel nedenlere dayanmaktadır. Çelişkilerin ekonomik olduğunu iddia eden Primakov, Sovyet sisteminin bilimsel ve teknik gelişmelere uyum sağlamakta yetersiz kaldığını da ifade etmektedir (Primakov, 2010:1-13). Primakov, çok kutuplu sistemi savunmaktadır ve Rusya'nın bunu gerçekleştirmesi gerektiğine inanmaktadır. Bu sebeple aralarında Çin ve Hindistan'ın da yer aldığı çok kutuplu sistemin oluşmasında çaba gösterilmesi gerektiğini ifade etmekte, Rusya'nın tek başına ABD'ye kafa tutmaması gerektiğini belirtmektedir. Primakov ayrıca eski Sovyet cumhuriyetleri ile ittifaklar kurulması, NATO'nun genişlemesine muhalefet edilmesi ve ABD önderliğindeki uluslararası sistemin zayıflatılması gerektiğine inanmaktadır (Rumer, 2019:2).

Putin'in göreve gelmesinin ardından yayınlanan Ulusal Güvenlik konseptinde, çok sayıda devletin ekonomik ve siyasi konumlarını güçlendirdiği ve ekonomik, politik, ekolojik ve bilgi faktörlerinin gün geçtikçe büyük rol oynadığı, bu durumun Rusya'nın çok kutuplu küresel sistemi sağlayabilmek için zemin oluşturduğu ifade edilmiştir. Rusya'nın dünya politikasında zayıflamasına karşılık askeri ve politik etkisi güçlenen NATO'nun doğuya doğru genişlemesi bunları engellemek için ise tehditlerin bir an önce tanımlanarak tehditleri önleyici planların geliştirilmesinin gerekliliği ortaya konulmuştur (National Security Concept of the Rusian Federition, 2020). Haziran ayında kabul edilen dış politika konseptinde ise ülke güvenliğinin ve toprak bütünlüğünün sağlanmasının yanında uluslararası sistemde Rusya'nın çıkarları ile uyumlu siyasi, ekonomik, entelektüel ve manevi potansiyelin güçlendirilmesi savunulmaktadır. Aynı zamanda Dünya kamuoyuna Rusya'nın temel sorunları, dış politika girişimleri ve eylemleri ile Rusya'nın faaliyetleri hakkında doğru bilgiler vermek, uluslararası alanda Rusya'ya karşı olumlu algı oluşturmak ve dostane tutum geliştirmek hedeflenmiştir (The Foreign Policy Concept of the Russian Federation, 2020). 2007 yılında Putin'in Münih Güvenlik Konferansında yaptığı konuşma Rusya'nın küresel politikada elde etmek istediği konuma ışık tutmaktadır. Konuşması boyunca Putin; Rusya'nın barış içinde yaşamak istediğinden ancak bunun gelişmesine izin vermeyen düşmanların bulunduğundan bahsetmiştir. Bu fikir Rusya'ya temel tehdidin Batı'dan geldiğini göstermektedir (Perrier, 2014:33). Küresel sistemde yükselen güçlere BRICS ülkelerinin ekonomik kapasiteleri üzerinden örneklendiren Putin, bunun kaçınılmaz olarak politik sonuçlarından bahsetmiş, NATO'nun sınırlarında bulunmasından duyduğu rahatsızlığı ifade ederek bu durumu provokasyon olarak nitelendirmiştir (Vladimir Putin 2007 Munich Speech, 2007).

2008-2012 yılları arasında Medvedev'in ardından yeniden devlet başkanı seçilen Putin, 2013 yılında yayınlanan dış politika konseptinde 21. yüzyılın ilk on yılında küresel alanda değişimlerin hızlı olduğu, Batı'nın ekonomisi ve siyasetini sistemde hakim kılabilme yeteneğinin Doğu'ya kaydığı gibi analizlerin yanında dış politika hedeflerine erişebilmek için yumuşak gücün uluslararası ilişkilerin vazgeçilmesi olduğu ve sivil toplum, bilgi, kültürel yöntemler ile teknoloji üzerine inşa edilecek dış

politikanın yumuşak güç ile harmanlanmasından bahsedilmektedir. Bunu sağlayabilmek için ise yurtdışındaki halklara yönelik Rus bilgi araçlarının geliştirilmesi, Rus kitle iletişim araçlarının uluslararası bilgi ortamındaki rolünün güçlendirilmesi ve bunun için devletin gerekli desteği sağlaması, devlet egemenliğine ve güvenliğine yönelik bilgi tehditlerini engellemek için önlemlerin alınması ve bunları yaparken yeni bilgi iletişim teknolojilerin sunduğu fırsatların yaygın olarak kullanılmasını benimsemiştir (Concept of the Foreign of the Russian Federation, 2013). Bu doktrin, Rusya'nın günümüzde pratikte uyguladığı stratejinin teorik çerçevesini ortaya koyarken günümüz dezenformasyon politikalarının pratiğe uygulanabilecek çerçevesi Genel Kurmay Başkanı Valeri Gerasimov tarafından ortaya koyulmuştur. "Önceden Hesaplamada Bilimin Değeri" adlı makalesinde 21. yüzyılda savaş ve barış arasındaki sınırın bulanıklaştığını, ilan edilmeden başlayan savaşların başladıktan sonra belirli şekillerde değil, bilinmeyen yöntemlerle ilerlediğini ve değişen savaş kurallarında stratejik hedefe ulaşmak için sivil araçların kullanımının ve öneminin arttığından bahsetmektedir. Gerasimov'a göre uygulanacak yöntemlerin ortak noktası nüfusun protesto potansiyeli koordineli olarak siyasi, ekonomik, enformatif, insani ve askeri olmayan yöntemleri birlikte kullanılmasını gerektirmektedir. Asimetrik olmayan uygulamalar silahlı çatışmaları sırasında karşı tarafın avantajlarını etkisin hale getirmeye yarayacak şekilde yaygın olarak kullanılmaktadır. Bu eylemler arasında düşman tarafın topraklarında kalıcı cephe oluşturabilmek için muhalefetin kullanılması ile sürekli geliştirilen enformatif eylemler aygıtlar ve araçlar önemlidir ('Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows, 2013).

2016 yılındaki enformasyon doktrininde Rusya bilgi güvenlini birey, toplum ve devletin iç ve dış bilgi tehditlerine karşı korunması olarak tanımlamaktadır. Doktorinde Rusya'nın egemenliğinin devamını sağlamak, toprak bütünlüğüne aykırı hareketler için bilgi ve psikolojik araçların gün geçtikçe daha yoğun kullanıldığı belirtilmekte ve bu faaliyetlerde dini, etnik, insan hakları ve diğer kurulların dahil olduğunu ve nihayetinde bilgi teknolojilerinin bu amaçla her geçen gün daha yoğun kullanıldığı vurgulanmaktadır. Yabancı medya organlarının Rusya politikalarına yönelik ön yargılı materyallerini yayınlama eğiliminde oldukları belirtilen doktrinde Rusya'nın kitle iletim araçları ve Rus gazetecilerin engellendiği Rus ahlak ve manevi değerlerini aşındırmak için Rusya ve Rus gençliği üzerinde baskı olduğu ifade edilmiştir (Doctrine of Information Security of the Russian Federation, 2016). Rusya'nın enformasyon alanında yaptığı durum tespitinde ve Rusya'ya yönelik gördüğü tehditlerde kendi uyguladığı enformasyon politikalarının izlerini bulmak mümkündür. Rusya uygulandığını iddia ettiği politikalardan birçoğunu devlet olarak benimsemiştir. Doktrinlerde belirlediği politikalara yönelik anlatılarını enformasyon alanında savunmakta, karşı anlatıyı ise zayıflatmaya çalışmaktadır.

6. ÖRNEK OLAY ANALİZİ: 2016 ABD BAŞKANLIK SEÇİMLERİNDE RUS MÜDAHALESİ

Sovyetler Birliği'nin beyaz, gri ve siyah propaganda/dezenformasyon yaklaşımında beyaz yöntem; bilinen bir kaynaktan yapılan bir dezenformasyon türü olarak

tanımlanmaktadır. Örneğin Kremlin'e bağlı olduğu bilinen medya kanalları tarafından yapılan dezenformasyon bu kapsamda değerlendirilmektedir. Gri yöntem ise kaynağı belirsiz olan paravan olarak oluşturulan, Rusya'nın düşmanlarını eleştirmekle birlikte, resmi olarak Rusya/Sovyetler Birliği ile bağlantılı olmayan yöntemle yapılan dezenformasyon türüdür. Siyah dezenformasyon ise kasıtlı olarak aldatmak üzerine kurgulanmış dezenformasyon türüdür (Cull vd, 2017).

2016 ABD seçimlerinde Rusya'nın beyaz dezenformasyonunun ayağını Rusya'ya bağlı medya kanalları olan Russia Today (RT) ve Sputnik oluşturmuştur. RT ve Sputnik; Rusya'nın Batı demokrasilerine yönelik yaklaşımı olan, Batı toplumlarının demokratik yönetişime olan güvenlerini sarsmak, ülke içinde bölücü siyasi kırılmaları kışkırtmak ve şiddetlendirmek, toplum ile seçilmişler arasındaki güveni aşındırmak, Rusya'nın politika gündemini diğer toplumlar arasında yaygınlaştırmak, gerçek ve kurgu arasındaki çizgiyi bulanıklaştırarak bilgi kaynakları arasında genel güvensizlik ve kafa karışıklığı yaratmayı amaçlamaktadır (Weisburg, 2016).

Rusya'nın iç ve dış politika anlatısını uluslararası kamuoyuna anlatmak için 2005 yılında kurduğu Russia Today, 2013 yılında dönüşüme uğramıştır. 2013 yılında Putin tarafından imzalanan kararla RT dahil olmak üzere devlet tarafından işletilen medya kanallarına yönelik bütçe kesintisi yasaklanmıştır (Elswah ve Howard, 2020). Sputnik kanalı ise 2014 yılında Federal Devlet Kurumu olarak bilinen "Rossiya Sgednya" ya bağlı olarak kurulmuş ve 30'dan fazla dilde yayın yapmaktadır (Köktürk,2020). RT ve Sputnik gibi kanallar formatları gereği haber kanalı gibi gözükse de doğrulanmış haberlerden ziyade bilgi-eğlencede dahil olmak üzere paylaşılan haberlerin dezenformasyon karıştırılarak verilmesidir. Bu kanalları diğer haber kaynaklarında verilen haberleri yanlış anlatmakta veya bir yalanın kaynağı olarak daha güvenilir kaynak göstermektedir (Paul ve Matthews, 2016). Bu medya kanallarının yayın politikaları kamu diplomasisi, propaganda ve geleneksel gazetecilik arasındaki çizgileri bulanıklaştırırken bu iletişim yönetişiminde dezenformasyona dayanan ancak bununla da sınırlı kalmayan içerikleri duygusal anlatılarla çekici hale getirmektedir (Wagnsson, 2022). Putin, benimsediği "dikey güç" konseptini iktidara gelmesinin ardından uygulayabilmiş ve medya kanallarını bu kapsamda Kremlin'e bağlamıştır (Öney,2017).

2016 yılında ABD'de gerçekleştirilen başkanlık seçimlerinde Rusya'nın siber müdahalede bulup, sonuçları etkilediği bilinmektedir (Ünver, 2019). ABD seçimlerine beyaz müdahale kapsamında değerlendirilecek beyaz faaliyetler kapsamında değerlendirilecek medya hareketlerine Rusya seçimlerden önce başlamıştır. Düşük yoğunluklu müdahalenin parçası olan RT, 2008 yılında ABD seçimleri sırasında yayında olan RT 2009 yılında yeni ve güçlü bir platform olarak kendini tanıtmış ve RT harflerini markalaştırarak Al Jazeera, CNN ve Fox News gibi alternatif kanal olarak kendini konumlandırmıştır. Ana akım çizgide devam eden yayınlar zaman zaman Rus çıkarını destekleyen hikayelerle verilmiştir. RT'nin asıl faaliyet sebebi Suriye olayları sırasında, Suriye rejimini destekleyen haberleri ile kendini göstermiştir. 2012 yılında ABD seçimlerinde Youtube'da 1 milyon görüntülemeye ulaşan RT aynı zamanda 450.000 abonesi ile izleyici kitlesini

geliştirmiş ve sosyal medyadaki varlığını artırmıştır. Seçimler sırasında dezenformasyon haberlerinin etkinliğini artırmak ve haberleri daha geniş kitleye duyurabilmek için internet ve sosyal medyayı kullanmak için Sputnik ile ortak çalışmıştır (Clapper ve Brown, 2018, s. 330). Çeyrek milyon dinleyiciye sahip RT televizyon ağı, komplo teorileri ve dezenformasyon faaliyetleri ile harmanlanmış haberler ile ABD'deki sorunları, sosyal ve politik gerilimleri artıracak şekilde Rus tercihlerine göre şekillendirerek haberleştirmiştir. Clinton hakkında olgusal veya üretilmiş olumsuz haberler yayılmıştır (Prier, 2020).

2017 ABD istihbaratı raporuna göre RT ve Sputnik ön seçim ve genel seçimlerde gün geçtikçe Trump lehine olumlu haberleri artırırken Clinton aleyhine olumsuz yayınlar yapmıştır. Özellikle, Clinton'ın sızdırılan e-postalarına odaklanan (malenformasyon), onu yolsuzluk, fiziksel ve zihinsel sağlığı yerinde olmayan ve İslami aşırıcılıkla suçlayan yayınlara odaklanılmıştır (Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent, dni, 2017).

Gri faaliyetler kapsamında seçim sürecinde insanların bilgileri doğrulayabileceği alan olan Wikileaks kullanılmıştır. Seçim sürecinde Wikileaks'e manipüle edici bilgiler girilmiş ayrıca CIA Direktörü Pompeo'ya göre hacklenmiş bilgiler yine Wikileaks'e girilmiştir (Isachenkov, 2017). Sadece bu bilgilerin girilmesi değil aynı zamanda kullanılan metodoloji Wikipedia'in Rusya tarafından gri alan faaliyetleri için kullanılmasına neden olmuştur. Hillary Clinton e-postalarını tek bir seride vermek yerine görünürlüğün artırılması, daha yaygın görülmesi ve daha kalıcı olması için bilgiler seri olmayan şekilde her yayın için ayrı hashtag kullanılarak yaygınlaştırılmış ve bu strateji etkili olmuştur. Yapılan çalışmalar Wikileaks'in seçili bilgileri Trump lehine kullanmak için metodolojik yaklaşım sergilendiğini göstermektedir (Proferes ve Summers, 2019). Doğrudan Rusya ile bağlantısı bulunmamasına rağmen seçili haberlere metodolojik yaklaşarak seçimlerin etkilenmeye çalışılması Wikileaks faaliyetlerinin gri alanda değerlendirilmesine neden olmaktadır.

Rusya'nın desteklediği (Whyte ve Etudo, 2020: 100) İnternet Araştırmaları Ajansı (Internet Research Center) 2016 seçimlerinde siyah alan faaliyetleri yürütmüştür. 2014-2017 yılları arasında İAA, sosyal medyada ABD'deki tartışmalarda Amerikalılar gibi davranan binlerce Twitter hesabı oluşturmuş ve kullanmıştır. Bu kampanyalar ise 2014 yılında başlamış ve 2016 yılındaki seçimlere zemin oluşturulmuştur (Lukito vd., 2020). Yapılan çalışmalar, İAA'nın ABD seçimlerinde kutuplaşma yaratmak ve ABD seçim kampanyası sırasında sıradan ABD vatandaşlarının oy verme tutumlarını etkilemek için ABD'li kullanıcıları taklit eden hesapları kullandığını tespit etmiştir (Bastos ve Farkas,2019). Kampanyalar Trump'ın kazanmasına odaklanırken genel anlamda ABD demokrasisini zayıflatmayı amaçladığı da ortaya çıkmıştır. Botlar ve trollerin faaliyetleri ise dezenformasyonun yayılması için kullanılmıştır (Weiss,2021:181-182).

İAA bu kampanyayı farklı sosyal medya platformlarında yürütebilmiştir. 3 vardiyalı çalışan ajans çalışanları asgari sayıda dezenformasyon üretmekte (blog yazısı, tweet vs), geri bildirimlerle gönderileri kalitelerini artırmaktaydılar ((Lukito vd., 2020). IRA

aynı zamanda troll çiftliği olarak da bilinmektedir. Twitter'a göre (Bertrand,2017), ABD seçim sürecinde IRA bağlantılı hesaplardan bazıları otomatik mesaj atarken bazıları kullanıcı mesajları atmıştır. 2752 hesabın attığı tweetlerin %9'u seçimle ilgili olduğunu ve bu tweetlerin %47'den fazlasının otomatik olduğunu ifade etmiştir. Bunun yanında Facebook ve Reddit gibi farklı sosyal medya hesapları da aktif olarak kullanılmıştır.

Nihai olarak dezenformasyon döngüsü; RT ve Sputnik taraflı haberle yayın yapmakta, manipüle edilmiş hacklenmiş bilgiler Wikipedia'ya yüklenmekte, ABD vatandaşı gibi davranan hesaplar, troller ve botlar bu haberlere link vererek sosyal medya hesaplarında paylaşmaktadır. Sonuç olarak ABD seçimlerinde dezenformasyon yapılması geniş bir stratejik kurgu içermektedir.

7.TARTIŞMA

Siber uzayın devletlerin dış politika amaçlarını gerçekleştirmek için kullanılmasıyla bir alan haline gelmesi siber müdahale kavramının kullanımını gerektirmektedir. Dış politika hedeflerinin gerçekleştirilmesi için devletler siber alanda kimliği açık veya gizli şekilde faaliyetler gerçekleştirmektedir. Rusya siber alanda etkili aktörlerden biridir ve siber alanı hibrit mücadeleyi farklı yöntemlerle kullanabileceği bir mecra olarak görmektedir. Dezenformasyon bu yöntemlerden biridir. Rusya'nın dezenformasyon uygulama yöntemi ise Sovyetler Birliği döneminden gelmektedir ve bilgi ekosisteminde etkin olunması gerektiğine yönelik doktrinlerle günümüzdeki uygulama çerçevesi çizilmiştir. Çalışmada Sovyetler Birliğinde uygulanan Beyaz, Gri ve Siyah propaganda/dezenformasyon sınıflandırmasını yaptığı iddia edilmektedir. Rusya 2016 ABD seçimlerinde dezenformasyonu yayacak ve etkili kılacak çok farklı yöntemler uygulamıştır. Çalışmada bu yöntemlerin sınıflandırılarak Sovyetler Birliği döneminde uygulanan yöntemler olduğu tespit edilmiştir.

8.SONUÇ

Bu çalışmada siber uzayın devletler açısından bir mücadele alanı olduğu ve dezenformasyonun bu mücadele alanında kullanıldığı 2016 ABD Başkanlık Seçimleri örneğinden hareketle incelenmiştir. Siber uzay gün geçtikçe internet aracılığıyla yaygınlaşmaktadır. Uydular aracılığıyla internet erişimi projeleri (Starlink), optik kablolarla erişim sağlanan internete erişiminin yakın gelecekte coğrafya fark etmeksizin tüm dünyaya yayılacağı anlamına gelmektedir. Buradan hareketle internet kullanıcı sayısının artmaya devam edeceğini söylemek mümkündür.

Uluslararası ilişkilerde devletler nihai olarak dış politika hedeflerine ulaşmak istemektedir. Bu yüzden farklı araçlar kullanılabilmektedir. Bu çerçevede siber uzay zaman içinde devletlerin dış politika hedeflerine ulaşmak için kullandıkları alan olmuştur. Uluslararası ilişkilerde siber hukuka yönelik kapsayıcı normun bulunmaması ve devletlerin yaptıkları müdahalelerde kendilerini gizleyebilmeleri siber alanı hibrit mücadelenin alanlarından biri yapmıştır. Siber alan günümüzde hibrit

mücadelenin parçası olarak çeşitli şekillerde kullanılmaktadır. Bu kullanım alanlarından biri de bilgi ekosistemine yapılan müdahaledir.

Bilgi ekosistemine yapılan müdahaleleri bilgi düzensizliği olarak da adlandırılabilir. Bilgi düzensizliği yöntemleri; dezenformasyon, mezenformasyon ve malenformasyondur. Dezenformasyon bilginin kasıtlı olarak yanıltıcı şekilde düzenlenmesi ve yayılmasıdır. Bu sebeple bunu gerçekleştirenin bir amacı olduğu ifade edilebilir. Devletlerin dezenformasyon kullanmasının ardında uzun vadeli stratejilerine ulaşmak için taktik seviyede uyguladıkları adımlar bulunmaktadır ve devletler bu alanı aktif olarak kullanmaktadır. İnternetin oluşturduğu bilgi ekosisteminde devletlerin aktif olarak bu alanı kullanmaya devam edeceği ifade edilebilir.

Bu bağlamda çalışmada, örnek olay analizinde gösterildiği gibi bilgi düzensizliği türlerini en çok kullanan ülkelerden olan Rusya, Sovyetler Birliği döneminden gelen tecrübeleri ABD başkanlık seçimleri döneminde amacına uygun olarak pratiğe dökmüştür. Sonuç olarak, Batı ile Rusya arasındaki tarihi rekabet günümüzde devam ederken, rekabet alanı ve yöntemleri siber alanda özellikle bilgi operasyonları bağlamında genişlemiştir. Önemli siyasi sonuçları olması bakımından Uluslararası İlişkiler ve Uluslararası Güvenlik Çalışmalarında dezenformasyon kavramının farklı boyutlarıyla daha çok çalışılması gerekmektedir.

DISINFORMATION AS A METHOD OF CYBER INTERVENTION IN RUSSIAN FOREIGN POLICY

During the Cold War, the competition between the USA and the USSR resulted in the creation of the internet, which is now embraced by every state according to its own narrative. While the USA advocates for the use of the internet worldwide within the framework of freedom and democracy, portraying it as a tool of neoliberal policies, China utilizes internet and infrastructure tools to strengthen its authoritarian regime. Meanwhile, Russia effectively employs its own internet and social media channels in the former Soviet Union territories while also using the internet and social media to undermine the narrative of the West. Thus, the internet is also a political arena. Access to the internet is increasing daily, presenting an important opportunity for states wishing to influence broader masses. People can instantly access global developments through social media channels, making social media a platform for states aiming to reach mass audiences.

With the expansion of the internet, cyberspace has become crucial, prompting states to compete in achieving their foreign policy objectives. The 2008 Estonian cyberattacks, the 2010 Arab Spring uprisings, and interventions in the 2016 US elections indicate the states' acknowledgment of cyberspace as a domain. Indeed, at its 2016 Warsaw Summit, NATO recognized cyberspace as a domain to be contested, akin to land, sea, air, and space. The significance of acknowledging cyberspace as a contested domain lies in Russia's utilization of cyberattacks and manipulation of the social media information ecosystem. Russia not only engages in disinformation campaigns in regions it intervenes in, such as Georgia and Ukraine but also effectively

utilizes disinformation in social media within NATO countries. Mainly during elections in democratic countries, Russia engages in disinformation campaigns to weaken the narrative of Western democracies and promote its own.

States utilize the cyber domain not only through cyberattacks or cyber espionage activities but also by intervening in the information ecosystem created by social media. Disinformation is one of the methods used by states, terrorist organizations, corporations, or individuals to influence the information ecosystem. These actors may engage in disinformation for their foreign policy objectives, ideologies, or financial gains. The widespread discussion of disinformation in international relations today stems from states' effective utilization of disinformation during crises (such as wars or elections) as part of their strategic communication.

States employ military, economic, and diplomatic methods to achieve their foreign policy objectives. In contemporary times, cyber intervention has become one of the methods used to realize foreign policy objectives. Cyberattacks, cyber espionage, and information disorder methods should be considered as forms of cyber intervention. Drawing from Rosenau's definition, cyber intervention should be understood as a disruptive action with a beginning and an end, applicable to temporary situations. Information disorder methods such as disinformation, misinformation, and malinformation can be employed as intervention tools. Countries engaging in intervention utilize these methods through social media to influence the information ecosystem of target countries.

Russia is one of the countries that is effectively utilizing cyber intervention methods. The 2008 Estonian cyberattacks, cyber interventions during the annexation of Crimea in 2014, and methods used during the 2016 US Presidential Elections are among Russia's cyber intervention tactics. Russia's success in the annexation of Crimea can be attributed to its combined use of conventional and unconventional hybrid methods. It can be argued that the disinformation tactics employed during the 2016 US elections also successfully influenced public opinion. Numerous reports within the US system have confirmed Russia's engagement in disinformation during elections. Furthermore, studies by think tanks and academics corroborate Russia's involvement in disinformation during elections. Disinformation is recognized in international literature as a method of hybrid warfare. Therefore, states are researching effective strategies to counter the asymmetry created by disinformation.

This study aims to investigate Russia's disinformation methods and cyber intervention tactics. Within this research, the methods used during the 2016 US Presidential Elections have been selected as a case study. The main argument of the study is that Russia utilizes the white, grey, and black propaganda methods used during the Soviet era within the framework of disinformation activities today. Russia has not only disseminated disinformation through Sputnik and RT. Still, it has also employed various methods, such as different internet sites and various troll armies, to ensure the effectiveness of disinformation. Therefore, understanding Russia's disinformation strategy through the lens of the 2016 US elections is essential for comprehending the

methods Russia may apply to other countries. The study has categorized Russia's disinformation methods during the 2016 US elections within the white, grey, and black areas, which have been validated by the selected case study of the 2016 US elections.

KAYNAKÇA

Bağbaşlıoğlu, A. (2021). Uluslararası Güvenlik ve Uluslararası Örgütlenme Üzerine Bir Değerlendirme. A. Bağbaşlıoğlu (Ed.), *Uluslararası Güvenlik ve Uluslararası Örgütler: Kavramlar, Yaklaşımlar ve Kurumlar* içinde, (s.3-26). Ankara: Nobel Yayınları.

Bastos, M., ve Farkas, J. (2019). "Donald Trump is my President!": The Internet Research Agency Propaganda Machine. *Social Media+ Society*, 5(3), 1-13.

Benkler, Y., Faris, R., ve Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American Politics*. Oxford University Press.

Bentzen, N. (2018). Online Disinformation and the EU's Response. European Parliamentary Service. Erişim adresi: https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf

Bertrand, N. (2017, October 30). Twitter will Tell Congress that Russia's Election Meddling was Worse than We First Thought. Business Insider. https://www.businessinsider.sg/twitter-russia-facebook-election-accounts-2017-10/

Bıçakçı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler Dergisi*, 10(40), 101-130.

Brantly, A. F. (2020). A Brief History of Fake: Surveying Russian Disinformation from the Russian Empire through the Cold War and to the Present. C. Whyte, A. Trevor Thrall ve Brian M. Mazanec (Ed.), *Information Warfare in the Age of Cyber Conflict* içinde, (s.27-41). London: Routledge.

Clapper, J. R., ve Brown, T. (2018). *Facts and Fears: Hard Truths from a Life in Intelligence*. New York:Viking.

Cohen, J., ve Fontaine, R. (2020). Uniting the Techno-Democracies. *Foreign Affairs*, October. Erişim tarihi: 20.10.2022. https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies

Concept of the Foreign Policy of the Russian Federation. (2013, February 12). https://thailand.mid.ru/en/concept-of-the-foreign-policy-of-russia

Cull, N. J., Gatov, V., Pomerantsev, P., Applebaum, A., ve Shawcross, A. (2017). *Soviet Subversion, Disinformation and Propaganda: How the West fought against It*. London: LSE Consulting.

Çelik, Ş. (2013). Stuxnet saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), 137-175.

Çoban, F. (2016). The Role of the Media in International Relations: from the CNN Effect to the Al-Jazeera Effect. *International Relations,* 4(2),45-61.

Denk, E. (2007). Medya ve Uluslararası Politika, *Uluslararası İlişkiler Dergisi*, 4(13), 145-156

Ellehuus, R. (2020, Ocak). Mind the Gaps: Russian Information Manipulation in the United Kingdom. CSIS. Erişim adresi: https://www.csis.org/analysis/mind-gaps-russian-information-manipulation-united-kingdom

Elswah, M., ve Howard, P. N. (2020). "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT). *Journal of Communication*, 70(5), 623-645.

Erdoğan, İ. (2013). Dördüncü Güç Medyadan Beşinci Güç İnternete: Demokratik Bir Dönüşüm mü Yaşanıyor? *Selçuk İletişim*, 8(1), 176-191.

Erlich, A., ve Garner, C. (2023). Is pro-Kremlin Disinformation Effective? Evidence from Ukraine. *The International Journal of Press/Politics*, 28(1),5-28.

Fallis, D. (2015). What is Disinformation? *Library Trends*, 63(3), 401-426.

Francois, C., ve Lin, H. (2021). The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot. *Journal of Cyber Policy*, 6(1), 33-57.

Georgia-Russia Conflict (2008). Cyber Law and Security Repository. Erişim adresi: https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008)

Gerasimov, V. (2013, Şubat 27). The 'Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows. Erişim adresi: https://inmoscowsshadows.wordpress.com/2014/07/06/thegerasimov-doctrine-and-russian-non-linear-war/

Hamzaoğlu, H. (2020). Rus Dış Politikasında Realist Yaklaşım: Primakov Doktrini ve Yakın Çevre Kavramı. *Avrasya Uluslararası Araştırmalar Dergisi*, 8(24), 281-299.

Hansen, I., ve Lim, D. J. (2019). Doxing Democracy: Influencing Elections via Cyber Voter Interference. *Contemporary Politics*, 25(2), 150-171.

Haslam, J. (2015). *Near and Distant Neighbors: A New History of Soviet Intelligence*. New York: Farrar,Straus and Giroux.

Hicks, K. H., ve Friend, A. H. (2019). By Other Means Part I: Campaigning in the Gray Zone. Center for Strategic & International Studies. Erişim adresi: https://apnews.com/article/8b7532462dd0495d9f756c9ae7d2ff3c

https://afyonluoglu.org/PublicWebFiles/strategies/Asia/Russia%202016%20Information%20Security%20Doctrine.pdf

Isachenkov, V. (2017, February 22). Russia Military Acknowledges New Branch: Info Warfare Troops. AP News. Erişim adresi: www.apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c.

Isachenkov, V. (2017, Şubat 22). Russia Military Acknowledges New Branch: Info Warfare.

İstihbarat Topluluğu Değerlendirmesi, Son ABD Seçimlerinde Rus Etkinlikleri ve Niyetlerini Değerlendirme, 2017. Erişim adresi: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Jensen, B., Valeriano, B., ve Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, 42(5), 58-80.

Kostyuk, N., ve Brantly, A. (2022). War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation. *Contemporary Security Policy*, 43(3), 498-515.

Köktürk, M. (2020). Post-Truth ya da Mağaraya Dönüş. *Pasajlar Dergisi: Post-Truth Çağı*, 2(4), 35-55.

Landler, M., ve Gordon, M. R. (2014, July 9). NATO Chief Warns of Duplicity by Putin on Ukraine. The New York Times. Erişim adresi: https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html

Larson, E., et al. (2009). *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. Santa Monica: RAND Corporation.

Lukito, J. (2020). Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017. *Political Communication*, 37(2), 238-255.

Lukito, J., Suk, J., Zhang, Y., Doroshenko, L., Kim, S. J., Su, M.-H., Xia, Y., Freelon, D., ve Wells, C. (2020). The Wolves in Sheep's Clothing: How Russia's Internet Research Agency Tweets Appeared in U.S. News as Vox Populi. *The International Journal of Press/Politics*, 25(2), 196-216.

Mansell, R. (2012). *Imagining the Internet: Communication, Innovation, and Governance*. Oxford:Oxford University Press.

Mansoor, P. R. (2012). Introduction: Hybrid Warfare in History. W. Murray ve P. R. Mansoor (Ed.), *Hybrid Warfare in History* içinde,(s.1-14). New York: Cambridge University Press.

McCombie, S., Uhlmann, A. J., ve Morrison, S. (2020). The US 2016 Presidential Election & Russia's Troll Farms. *Intelligence and National Security*, 35(1), 95-114.

McCrory, D. (2020). Russian Electronic Warfare, Cyber and Information Operations in Ukraine. *The RUSI Journal*, 165(7), 34-44.

McCulloh, T., ve Johnson, R. (2013). *Hybrid Warfare*. Florida: Joint Special Operations University.

Merlingen, M. (2023). Coloniality and the Global North War Against Disinformation: the Case of the European Union. *Third World Quarterly*, 44(4), 744-761.

Moral, P. (2022). The Challenge of Disinformation for National Security. J. Cayon Peña (Ed.), *Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts*.içinde, (s.103-123). Berlin:Springer.

Morozov, E. (2012). *The Dark Side of Internet Freedom: The Net Delusion*. New York:Public Affairs.

National Security Concept of the Russian Federation. (2020, January 10). Erişim adresi: https://nuke.fas.org/guide/russia/doctrine/gazeta012400.htm

Öney, S. (2017). Kremlin Odaklı Medya: Kaotik Çoğulculuktan İstikrarlı Tekelciliğe/Tekelciliğe Rusya'da Medya. G. Özcan, E. Balta ve B. Beşgül,(Ed.), *Kuşku ile Komşuluk: Türkiye ve Rusya İlişkilerinde Değişen Dinamikler* içinde (s.299-320) İstanbul: İletişim Yayınları.

Perrier, E. M. (2014). The Key Principles of Russian Strategic Thinking. IRSEM, Institut de recherche stratégique de l'École militaire.

Pope, A. E. (2018). Cyber-Securing our Elections. *Journal of Cyber Policy*, 3(1), 24-38.

Potter, E. H. (2019). Russia's Strategy for Perception Management through Public Diplomacy and Influence Operations: The Canadian Case. *The Hague Journal of Diplomacy*, 14(4), 402-425.

Prier, J. (2020). Commanding the trend: Social media as information warfare. J. Arquilla ve J. A. Ronfeldt (Ed.), *Information Warfare in the Age of Cyber Conflict* içinde, (s. 88-113). London:Routledge.

Primakov, Y. (2010). *Rusyasız Dünya*. Ankara:Timaş Yayınları.

Proferes, N., ve Summers, E. (2019). Algorithms and Agenda-setting in Wikileaks' #Podestaemails release. *Information, Communication & Society*, 22(11), 1630-1645.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare. Farrar*, New York: Straus and Giroux.

Rumer, E. (2019). The Primakov (Not Gerasimov) Doctrine in Action. Carnegie Endowment for International Peace. Erişim adresi: https://carnegieendowment.org/2019/06/05/primakov-notgerasimov-doctrine-in-action-pub-79254

Savitz, E. (2012). 5 Things You Need to Know About Chinese Social Media. Forbes. Erişim tarihi: 20.07.2023. https://www.forbes.com/sites/ciocentral/2012/10/25/5-things-you-need-to-know-about-chinese-social-media/

Schmitt, N. M. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Schmitt, N. M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs*, 90(1), 28-41.

Snyder, A. A. (2012). *Warriors of Disinformation: How Lies, Videotape, and the USIA Won the Cold War*. New York:Arcade.

Starr, P. (n.d.). How Neoliberal Policy Shaped the Internet—And What to Do About It Now. Prospect. Erişim tarihi: 31.08.2022. https://prospect.org/power/how-neoliberal-policy-shaped-internet-surveillance-monopoly/

The Foreign Policy Concept of the Russian Federation. (2000, Haziran 28). Erişim adresi: https://nuke.fas.org/guide/russia/doctrine/econcept.htm

The Media Manipulation Casebook: Code Book (Version 1.0). (2020). Harvard Kennedy School Shorenstein Center on Media, Politics and Public Policy.

Thompson, E. M. (1991). Nationalist Propaganda in the Soviet Press. 1939-1941. *Slavic Review*, 50(2), 385-399.

Ünver, H. A. (2019). Türkiye'deki Rus Dijital Medya ve Bilgi Ekosistemi. Sy, 2019(2).

Vladimir Putin 2007 Munich Speech. (t.y.). Erişim adresi: https://www.youtube.com/watch?v=U4MAsIh3zMA

Wagnsson, C. (2022). The Paperboys of Russian Messaging: RT/Sputnik audiences as vehicles for malign information influence. Information, *Communication & Society*, 26(9), 1849-1867

Wardle, C. (2020). Bilgi Düzensizliği Çağı. C. Silverman (Ed.), *Dezenformasyon ve Medya Manipülasyonu Üzerine Doğrulama El Kitabı* içinde, (s.9-15). European Journalism Centre.

Weisburd, A., Watts, C., ve Berger, J. (2016, Kasım 6). Trolling for Trump: How Russia Is Trying to Destroy Our Democracy. War on the Rocks. Erişim adresi: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-todestroy-our-democracy/

Weiss, C. (2021). *The Survival Nexus: Science, Technology, and World Affairs*. New York:Oxford University Press.

Whyte, C., ve Etudo, U. (2020). Cyber by a Different Logic: Using an Information Warfare Kill Chain to Understand Cyber-Enabled Influence Operations. J. Arquilla ve J. A. Ronfeldt (Ed.), *Information Warfare in the Age of Cyber Conflict* içinde, (s.88-113), London:Routledge.

Whyte, C., ve Mazanec, B. (2018). *Understanding Cyber Warfare: Politics, Policy and Strategy*. London:Routledge.

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, 64(5), 7-26.

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections*, 15(2), 73-87.

Yin, R. K. (2003). *Case Study Research: Design and Methods*, California:Sage.

Zhao, B., et al. (2023). Manufacturing Conflict or Advocating Peace? A Study of Social Bots Agenda Building in the Twitter Discussion of the Russia-Ukraine War. *Journal of Information Technology & Politics*.21 (2),176-194.

KATKI ORANI / *CONTRIBUTION RATE*	**AÇIKLAMA / *EXPLANATION***	**KATKIDA BULUNANLAR / *CONTRIBUTORS***
Fikir veya Kavram / *Idea or Notion*	Araştırma hipotezini veya fikrini oluşturmak / *Form the research hypothesis or idea*	Yücel BAŞTAN/Filiz ÇOBAN ORAN
Tasarım / *Design*	Yöntemi, ölçeği ve deseni tasarlamak / *Designing method, scale and pattern*	Yücel BAŞTAN/Filiz ÇOBAN ORAN
Veri Toplama ve İşleme / *Data Collecting and Processing*	Verileri toplamak, düzenlenmek ve raporlamak / *Collecting, organizing and reporting data*	Yücel BAŞTAN/Filiz ÇOBAN ORAN
Tartışma ve Yorum / *Discussion and Interpretation*	Bulguların değerlendirilmesinde ve sonuçlandırılmasında sorumluluk almak / *Taking responsibility in evaluating and finalizing the findings*	Yücel BAŞTAN/Filiz ÇOBAN ORAN
Literatür Taraması / *Literature Review*	Çalışma için gerekli literatürü taramak / *Review the literature required for the study*	Yücel BAŞTAN/Filiz ÇOBAN ORAN