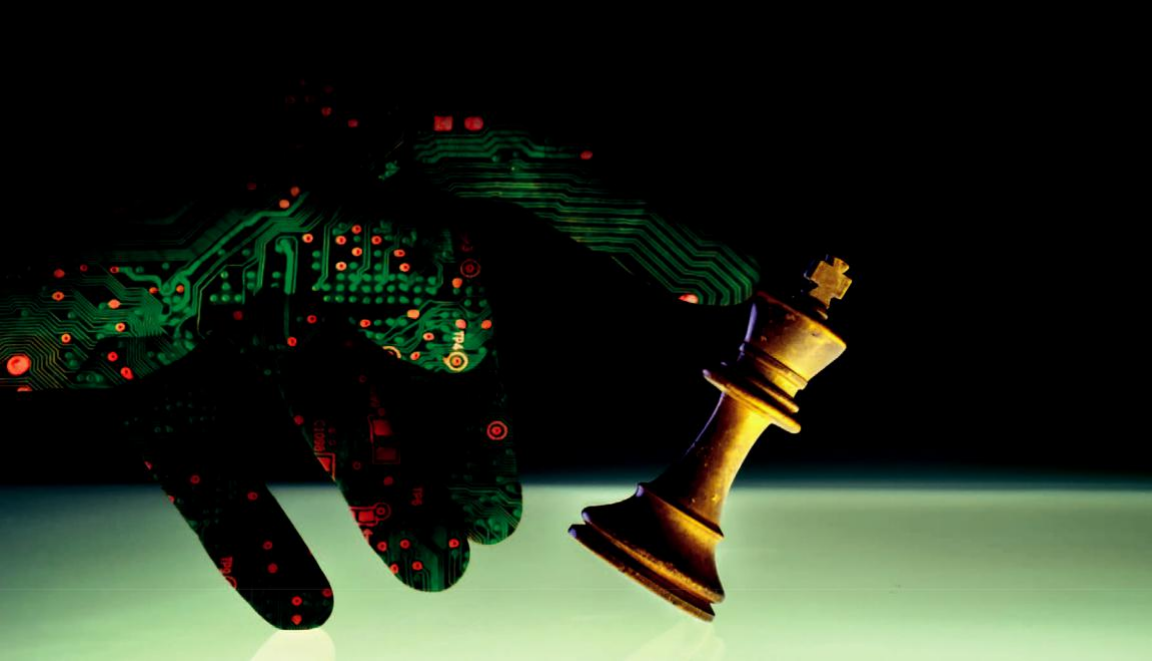




Ortaya Çıkan Risk Sanal Toplumda Savaş Ortamı

Değişimde Sosyal Manipölasyon ve
Bilgi Ortamı

Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey,
Sarah Anita Heintz, Luke J. Matthews



Bu yayın hakkında daha fazla bilgi için www.rand.org/t/RR2714 adresini ziyaret edin.

Library of Congress Yayında Kataloglama Verileri bu yayın için mevcuttur. ISBN: 978-1-9774-0272-1

RAND Corporation, Santa Monica, California tarafından yayınlanmıştır. © Telif Hakkı
2019 RAND Corporation **R**® tescilli bir ticari markadır.

Kapak: JohnDWilliams/iStock/Getty Images Plus.

Sınırlı Baskı ve Elektronik Dağıtım Hakları

Bu belge ve burada yer alan ticari marka(lar) kanunla korunmaktadır. RAND fikri mülkiyetinin bu temsili yalnızca ticari olmayan kullanım için sağlanmıştır. Bu yayının izinsiz olarak internette yayınlanması yasaktır. Değiştirilmemiş ve eksiksiz olduğu sürece, bu belgenin yalnızca kişisel kullanım için çoğaltılmasına izin verilir. RAND'ın herhangi bir araştırma belgesini ticari kullanım için çoğaltmak veya başka bir biçimde yeniden kullanmak için izin alması gerekir. Yeniden yazdırma ve bağlantı izinleri hakkında bilgi için lütfen www.rand.org/pubs/permissions adresini ziyaret edin.

RAND Corporation, dünya çapında toplulukları daha güvenli ve daha güvenli, daha sağlıklı ve daha müreffeh hale getirmeye yardımcı olmak için kamu politikası zorluklarına çözümler geliştiren bir araştırma kuruluşudur. RAND, kâr amacı gütmeyen, tarafsız ve kamu yararına kararlıdır.

RAND'ın yayınları, araştırma müşterilerinin ve sponsorlarının görüşlerini yansıtmayabilir.

RAND'ı destekleyin
Vergiden düşülebilir bir hayır kurumu katkısında bulunun
www.rand.org/giving/contribute

www.rand.org

önsöz

Bu analiz, sosyal manipölasyon teknikleri üzerine daha geniş bir çalışmanın parçası ve son zamanlarda Rusya'nın Batı bilgi ortamlarını manipöle etme çabalarıyla motive edildi. Bu çalışma, sosyal manipölasyon çabalarının geleceğine odaklanmakta ve birbiriyle örtüşen bilgi ile ilgili teknolojilerin ve bunların manipölasyon potansiyellerinin araştırılmasını içermektedir. Ortaya çıkan *sanal toplumsal savaş* olgusunu tanımlar ve Batı demokrasilerinin yanıt vermesi için yollar önerir.

Araştırma, Savunma Bakanlığı Ofisi olan Net Assessment Ofisi tarafından desteklendi ve RAND Ulusal Savunma Araştırma Enstitüsü'nün Uluslararası Güvenlik ve Savunma Politikası Merkezi bünyesinde yürütöldü. Savunma Bakanı Ofisi, Müşterek Kurmay, Birleşik Muharip Komutanlıklar, Deniz Kuvvetleri, Deniz Piyadeleri, savunma teşkilatları ve savunma İstihbarat Topluluğu.

RAND Uluslararası Güvenlik ve Savunma Politikası Merkezi hakkında daha fazla bilgi için bkz. <https://www.rand.org/nsrd/ndri/centers/ isdp.html> veya direktörle iletişime geçin (iletişim bilgileri web sayfasında verilmiştir).

İçindekiler

Önsöz	iii
Tablo	ix
Özet	xi
Teşekkür	xix
Kısaltmalar	xxi

BİRİNCİ BÖLÜM

Yeni Bir Çatışma Biçimi	1
Tanımlar ve Kavramlar	5
Yaklaşım ve Metodoloji	10

İKİNCİ BÖLÜM

Gelişen Bilgi Küresi	13
Daha Geniş Sosyal Eğilimler	14
Bilgi Dünyasında Eğilimler: Bilgi ve Farkındalık	18
Ağa Bağlı Dinamikler ve Bilginin Viral Yayılımı	21
Sansasyonizm	23
Bilgi Kaynaklarının Parçalanması	25
Bilgi Platformlarının Yoğunlaşması	28
Yankı Odalarının Rolü	29
Etkileyenlerin Rolü	35
Trollük Etiği	36
Veri Kuralı	38
Özet: İleri Düzey için Değişen Bir Bilgi Ortamı	
demokrasiler	40

ÜÇÜNCÜ BÖLÜM

Sosyal Bilimlerden İlgörüler	43
Tutumlar ve Tutum Değişimi	45
Tutumlar Değiştiğinde: Tutum Kayması Kriterleri	48
Dezenformasyonu Düzeltmek: Geri Tepme Etkisinin Ötesinde	55
Sosyal Güveni Etkileyen Faktörler	59
Tutumların Doğası ve Değişen Bilgi Küresi	62

BÖLÜM DÖRT

Gelişen Teknolojiler	65
Etkinin Hassas Hedeflemesi	67
Yapay Zeka	68
Algoritmik Karar Verme	72
Sanal ve Artırılmış Gerçeklik	75
Nesnelerin İnterneti	77
Ses Etkin Arayüzler	80
Blockchain ve Dağıtılmış Defter Sistemleri	83
Video ve Ses Sahtekarlığı	84
Gözetim Sistemleri	92
Sonuç: Hızla Değişen Bir Bilgi Dünyası	94

BEŞİNCİ BÖLÜM

Gelecek 1: Gerçekliğin Ölümü (2025 Senaryosu)	97
Metodoloji Üzerine Bir Not	97
Genel Gelecek	99
Sanal ve İcat Edilmiş Gerçekliğin Geleceği	104
Dünyanın Paylaşılan Bir Resminin Sonu	111
Gerçeğin Ölümünde Bilgi Saldırganlığı ve Manipölasyon	112

ALTINCI BÖLÜM

Gelecek 2: İnanç Siloları (2024 Senaryosu)	117
Genel Gelecek	117
Parçalanmış Bir Toplum	119
Silo Savaşları	122
Büyüyen Siber Taciz Manzarası	124
Bilgiye Dayalı Saldırganlık ve Silo Geleceği	128

YEDİNCİ BÖLÜM

Gelecek 3: Algoritmaların Yükselişi (2026 Senaryosu)	131
Genel Gelecek	131
Bilgi Bulutu	132
Etkileşimli Veri	136
Bulut, Nerede Olduğunuzu ve Ne Düşündüğünü Biliyor	140
Algoritma Tarafından Yönetilen: Papa'ya Teslim Olmak	142
Zafiyetler ve Riskler	147
Algoritmik Bir Gelecekte Bilgi Saldırganlığı	149

SEKİZİNCİ BÖLÜM

Sanal Toplumsal Savaşın Ortaya Çıkan Riski	153
Yeni Bir Çatışma Biçimi: Sanal Toplumsal Savaş	155
Sanal Toplumsal Saldırganlık Tehdidiyle Başa Çıkmak	161
Bir Yanıt Tasarlamak: İlk Gündem	163

Referanslar	171
--------------------------	------------

Tablo

4.1. Gelişen Sosyal Manipölasyon Teknolojileri ve Sanal Toplumsal Saldırganlık	66
---	----

Özet

sosyal manipölasyon olarak adlandırılabilir geniş bir fenomen-konularına ilgi patlaması yaşandı . Biz bu çalışmada bu kavramı , *bilginin amaçlı, sistemli bir şekilde üretilmesi ve yaygınlaştırılması olarak tanımlıyoruz. inançları, tutumları ve davranışları etkileyerek hedef bir ülkede zararlı sosyal, politik ve ekonomik sonuçlar üretmek için bilgi* . Örnekler Rusya'nın propaganda ve dezenformasyon yoluyla seçimleri etkileme ve Batı'da anlaşmazlık yaratma çabaları bu yükselen meydan okumadan; Facebook gibi sosyal medya platformlarının bu tür yanlış bilgilerin yayılmasındaki rolü; ve bölgesel anlatıları şekillendirmek ve belirli ülkelerde siyasi güç kazanmak için gelişen Çin programları. ABD istihbarat servisleri, Rusya'nın 2016 seçimlerini etkilemek için bu tür teknikleri kullandığı sonucuna vardı ve Moskova, ABD'de ve Avrupa'da - bazen ABD'nin uyarılarına rağmen yüzüstü - bunları kullanmaya devam ediyor.

Bu gelişmeler ne kadar önemli olsa da, saldırgan bir ulusun hedef ülkenin bilgi ortamını bozmak ve şekillendirmek için tasarlanmış teknikler ve teknolojilerle başarabileceklerinin yalnızca başlangıcını temsil edebilirler. Bu raporun birincil sonucu, sosyal manipölasyon çabalarının halihazırda önemli olduğu kadar, Amerika Birleşik Devletleri ve diğer demokrasilerin, bu yaklaşımların bir gün başarabileceklerine dair buzdağının yalnızca görünen ucunu görebildiğidir.

Yapay zekadan sanal gerçekliğe ve kişiselleştirilmiş mesajlaşmaya kadar ortaya çıkan birden çok teknolojinin kesişimi, saldırganların insanların temel sosyal gerçekliğini değiştirme potansiyeli yaratıyor. Bilgiyle ilgili iyi bilinen iki tehdit, büyük altyapı sitelerine yönelik klasik siber saldırılar ve internet destekli dezenformasyondur, ancak bu rapor arada gelişen manzaraya dikkat çekiyor - toplumun bilgi temelli temelinin ortaya çıkan ve kalıcı saldırılara karşı savunmasız olan alanları. bozulma ve manipülasyon. Özellikle “Nesnelerin İnterneti”nin (IoT) ve algoritmik ve büyük veriye dayalı karar vermenin yükselişiyle birlikte, gelişmiş toplumlar bilgi ve veri toplama, değiş tokuş, iletişim, analiz ve karar verme ağlarına tehlikeli bir şekilde bağımlı hale geliyor. Bu riskler , diğer eğilimlerin yanı sıra, otoritenin parçalanması, inanç silolarının yükselişi ve kalıcı bir “infosfer” ile karakterize edilen bilgi dünyasının (post-modern demokrasileri yöneten bilgi ortamı) *değişen* doğası nedeniyle bugün özellikle önemlidir. şekilsiz bir toplumsal muhalefet adına alaycı ve saldırgan taciz etiği.

Gelişmiş ekonomilerin vatandaşlarına zaten bir bilgi toplumunda yaşadığımızı hissettirse de, aslında bu dönüşümün sadece ilk ipuçlarını gördük. Ve bu geçiş, devlet ya da devlet dışı düşman rakiplerine bu toplumlara ulaşmak ve aksamalara, gecikmelere, verimsizliğe ve aktif zarara neden olmak için benzeri görülmemiş fırsatlar sunacak. Ülkeleri nesillerdir olduğundan daha kalıcı bir şekilde savunmasız hale getirecek sanal bir toplumsal saldırganlık biçimine kapı açacak. Bu tür sanal saldırganlık, ulusal güvenliğin karakterini ve onu korumak için atılan adımları yeniden düşünmeye zorlayacaktır.

Bilgiye dayalı sosyal manipülasyonun geleneksel biçimleri, inançları etkilemek için örneğin propaganda, kamu diplomasisi ve sosyal medya gönderileri aracılığıyla anlatıları yaymaya odaklanmıştır. Klasik düşmanca siber saldırılar, bankalar, elektrik santralleri veya santrifüjler gibi fiziksel hedeflere saldırmak için genellikle bilgi ağlarını bir otoyol olarak kullandı. Gelişmiş bilgi ortamlarının evrimi, hızla üçüncü bir olası saldırganlık kategorisini yaratıyor: ekonomik ve sosyal sistemlerin etkin işleyişinin bilgi temellerini manipüle etme veya bozma çabaları. Saldırganlar artacak-

Yalnızca dezenformasyonu veya olumlu anlatıları yayma veya fiziksel altyapıya zarar verme değil, aynı zamanda büyük veritabanlarının, algoritmaların ve bilgisayarlı, bilgisayarla geliştirilmiş veya bilgisayar bağımlı şeylerin ağlarının işleyişini çarpıtma ve zarar verme fırsatına sahip olurlar. modern toplumlar tamamen bağımlı olacaktır.

Sanal toplumsal savaş dediğimiz şey , aşağıdakiler de dahil olmak üzere çok çeşitli tekniklerin herhangi bir kombinasyonunu içerebilir:

- sosyal medya da dahil olmak üzere birden fazla kanal aracılığıyla klasik propaganda, nüfuz ve dezenformasyon operasyonlarını uygulamak
- paylaşılan gerçekliğe olan güveni azaltmak için büyük miktarlarda son derece makul fabrikasyon video ve ses materyali üretmek
- doğru ve yanlış bilgi arasında ayrım yapabilen kilit aracı kurumların itibarını sarsmak
- ekonominin ana bileşenlerinin giderek daha fazla güvendiği veritabanlarını bozmak veya manipüle etmek
- Algoritmik karar alma sistemlerini manipüle etmek veya küçültmek, hem günlük hükümet ve şirket operasyonlarını bozmak hem de kurumlara olan inanç kaybını yoğunlaştırmak ve ayrıca sosyal şikayetleri ve kutuplaşmayı artırmak için
- Kesinti ve hasar oluşturmak için patlayan IoT arasındaki bağlantılarda bulunan güvenlik açıklarını kullanmak
- Bozulma veya zihinsel ıstırap yaratmak veya belirli anlatıları güçlendirmek için sanal ve artırılmış gerçeklik sistemlerini ele geçirmek
- verimsizlik ve bazı durumlarda kişisel hayal kırıklığı ve endişe yaratmak için sohbet robotu tarzı etkileşimli sistemlere komutlar eklemek.

Çoğu durumda, bu tür bir saldırganlığın birincil amacı, fiziksel zarardan çok, kafa karışıklığı ve büyük sosyal kurumların işleyişinde hızlanan bir güven kaybı olmayabilir. Ve bilgiye bağımlı toplumların ortaya çıkması, saldırganların kullanabileceği sosyal manipülasyon teknikleri dizisini genişletecek ve derinleştirecek, bu da onların son derece uyarlanmış fiziksel hasar ve tutum değişiklikleri kombinasyonları

aramasına izin verecektir. Güvenin rolü bu analizde tutarlı bir temadır: Bilgi sistemlerinin etkin işleyişine yönelik saldırılar doğrudan saldırıdır.

toplumsal güven düzeylerinde, gelişmiş toplumların kurumlarına ve süreçlerine güvenilemeyeceği duygusu yaratmak ve kalıcı bir güvensizlik ve endişe duygusu yaratmak.

Bu tekniklerin nasıl gelişebileceğine ışık tutmak için RAND araştırmacıları, bu projeden Rusya ve Çin'in düşmanca sosyal manipülasyon çabalarına odaklanan bir birinci aşama analizini geliştirdiler. Bu proje henüz çözümlere yönelik değildi, daha çok anlamaya, yani ortaya çıkan zorluğun karakterini kavramaya yönelikti. Tehdide yönelik olası yanıtların daha ayrıntılı tartışılması için zemin hazırlamak üzere tasarlanmıştır. Ancak bu araştırma aşamasının bir dersi, bu eğilimlerin, teknolojilerin ve yeteneklerin birçoğunun yeterince anlaşılmadığı ve bazı olası yanıtların bilgi ortamının işleyişi, ifade özgürlüğünün karakteri ve diğer konular için potansiyel olarak dramatik etkileri olduğudur. Olası sonuçların titiz bir analizini yapmadan olası çözümleri ilan etmeye başlamak tehlikeli olacaktır. Bu rapor, öncelikle sorunun kapsamını ve yapısını analiz ederek bu tür çalışmalara zemin hazırlamak üzere tasarlanmıştır.

Sanal toplumsal savaş riskini anlamak için, bu tekniklerin gelecekte nasıl gelişebileceğinin bazı ilk hatlarını çizmek için bir dizi kategorideki kanıtları araştırdık. Değerlendirmeyi (1) Amerika Birleşik Devletleri ve diğer ileri demokrasilerdeki bilgi ortamının değişen karakterindeki eğilimler üzerine ayrıntılı araştırmalara dayandırdık; (2) tutumlar ve inançlar üzerine sosyal bilim araştırmalarının içgörülerini; ve (3) düşmanca sosyal manipülasyon uygulamalarına ve onun daha ayrıntılı ve tehlikeli kuzeni olan sanal toplumsal savaşa dayanan ilgili yeni teknolojilerdeki gelişmeler (Birinci Bölümde daha ayrıntılı olarak tanımlanan terimler). Her üç durumda da, yerleşik araştırma bulguları ve mevcut eğilimler hakkında veri topladık.

İkinci Bölüm, bilgikürenin özelliklerine ilişkin analizimizi sunar - bu tür düşmanca tekniklerin kullanılacağı bağlam. Üçüncü Bölüm, en etkili olabilecek sosyal manipülasyon biçimleri hakkında inanç ve tutumlara ilişkin araştırmaların neler önerdiğini araştırarak sosyal bilimlerden içgörüler elde eder. Dördüncü Bölüm, gelecekteki manipülasyon kampanyalarında rol oynayabilecek yapay zekadan sanal gerçekliğe ve IoT'ye kadar çeşitli teknolojilerdeki mevcut gelişmeleri incelemektedir.

Bu analizde benimsenen ikinci bir birincil yaklaşım, sosyal manipülasyon geleceklerinin olası şeklini tanımlamak için bir senaryo planlama metodolojisi kullanmaktır. Beşinci Bölümden Yedinci Bölüme kadar, eğilimler ve gerçekler üzerine araştırmanın bulgularına, Rus ve Çin sosyal manipülasyon stratejilerine ilişkin önceki çalışmanın içgörülerine ve diğer araştırmalara dayanarak, sosyal manipülasyonun nasıl etkileyebileceğine dair üç senaryo taslağını çiziyoruz. Önümüzdeki on yılda gelişmiş toplumlar. Üçü birbirini dışlayan değildir; her biri farklı bir temayı vurgular, ancak üçünün öğelerinin gerçek bir geleceği karakterize etmek için birleşmesi muhtemeldir. Her durumda, senaryoların farklı varsayımlarını desteklemek için kapsamlı araştırmalara atıfta bulunuyoruz ve her durumda, saldırgan sosyal manipülatörlerin avantaj elde etmek için bu senaryonun yönlerini nasıl kullanabileceğini açıklıyoruz.

Analiz, sanal toplumsal savaşın, birlikte bu yeni savaş biçiminin temel doğasını ve karakterini yansıtan birçok temel özelliğe sahip olmasının muhtemel olduğunu öne sürüyor. Bu özelliklerin tam olarak anlaşılması ancak zaman içinde ortaya çıkacaktır, ancak bu analiz, ortaya çıkan bu zorluğun tanımlanmasına yardımcı olabilecek ilk bir dizi özelliğe işaret etmektedir. Aşağıdakileri içerirler:

- *Ulusal güvenlik, giderek daha esnek bir bilgi ortamına ve daha da temel olarak güçlü bir “sosyal topografyaya” dayanacaktır.* bu Esnek bir bilgi küresinin unsurları iyi anlaşılmamıştır, ancak muhtemelen klasik bilgi güvenliği biçimlerinin yanı sıra güçlü aracı kurumları ve sürekli olarak sosyal manipülasyon tekniklerine karşı aşılınmış bir nüfusu içerirler.
- *Kamusal ve özel çabalar ve sorumluluklar arasındaki engel bulanıklaşıyor; ulusal güvenlik, kamu yatırımları kadar özel aktörlerin işbirliğine de bağlı olacaktır.* teknolojiler ve Bu tür bir çatışmanın teknikleri çok çeşitli aktörler için giderek daha fazla erişilebilir hale geliyor. Bu alandaki özel güç, bazı durumlarda kamu gücünü aşar ve aşar.
- *Çatışmalar giderek ağlar arasında ve ağlar arasında devam edecek.* Bu kalıbı, örneğin, Rusya tarafından bilgi kampanyalarının bir parçası olarak istihdam edilen bilgisayar korsanları, aktivistler ve gayri resmi propagandacıardan oluşan karmaşık, uluslararası ağda zaten görüyoruz.

ve Çin'in kilit anlatılar üzerindeki kontrolünü daha da artırmak için yurtdışındaki Çin vatandaşlarını ve etnik Çinlileri kullanması. Devlet aktörlerinin, atıf yapmaktan kaçınmak ve misillemeye karşı sanal toplumsal savaş yeteneklerini güçlendirmek için bu tür ağlar geliştirmesi muhtemeldir. Gölge bir küresel ağı anlamak, doğru bir portresini sürdürmek ve ona karşılık vermek çok daha zor olacak.

Bunlar, sanal toplumsal alanda çatışmayı yönetecek ilke türlerinin yalnızca ilk üç önerisidir. Bu alanı daha tam olarak anlamak ve demokratik toplumları en kötü etkilerine karşı koruyacak türde tepkileri anlamaya başlamak için acilen daha fazla araştırmaya ihtiyaç var. Sekizinci Bölüm, bu artan risk karşısında demokratik direnci artırmak için birkaç başlangıç tepki yoluna işaret ederek sona ermektedir. Bunlar aşağıdakileri içerir:

- *Araştırmaya ve anlamaya yatırım yapın* . Birçoğunda tutarlı bir tema Bu çalışma için yaptığımız konuşmaların ve analizlerin bir kısmı farkındalığımızın sınırları olmuştur: gelişen bilgi küresinin gerçek karakteri ve olası yönleri, bu evrimdeki temel nedensel dinamikler, popülasyonların çeşitli sosyal manipülasyon biçimlerine nasıl tepki verdiği ve en etkili olanın ne olduğu. cevaplar olabilir. Esnek bir bilgi küresinin ve sağlam bir sosyal topografyanın temel özellikleri nelerdir? Bu hedeflere ulaşip ulaşmadığımızı değerlendirmek için hangi metrikleri kullanabiliriz?
- *Bilgiye dayalı sosyal manipülasyonun en kötü biçimlerine karşı aşılama ve dayanıklılık biçimleri oluşturmaya başlayın* . Kampanyalar kendilerini dışarıdan gelen iddialara oluştuktan sonra karşı koymakla sınırlamazlar, bunun yerine bu tür iddialara ve kampanyalara karşı direnç oluşturmak için önceden adımlar atarlar. Önceden uyarı, yerleşik anlatıların sonradan ele alınmasından daha etkili olabilir.
- *Bugün sosyal medyanın oynadığı öncü rolü ve bu alanda devam eden bilgi kontrolü tartışmalarının çoğunun emsal oluşturan karakterini ciddiye alın* . Hükümetler, sosyal medya platformlarını sorunları mümkün olan en üst düzeyde çözmeye teşvik edebilecek eylemlere giderek daha fazla bakmalıdır. Bu süreçte, hükümetler dört ila beş şeyi tanımlamalıdır.

platformlar, soruna bir adım atmak için önümüzdeki iki ila üç yıl içinde yapabilir.

- *Amerikalıların olayları anlamlandırmasına yardımcı olabilecek yeni, geniş ölçüde güvenilen bilgi aracılık kurumları kurmak için tasarlanmış yatırımlar yapın* . Hükümetler (ayrıca özel vakıflar ve aktivistler) ayrıca internet tarayıcıları (özellikle yeni yaklaşımlarda öncülük etmeye istekli olanlar) gibi bilgi şirketleri arasında, gözden geçirilmiş algoritmalar, yeni tarayıcı uzantıları ve farklı siteleri ve kaynakları derecelendirmek ve sıralamak için deneme yanılma çalışmalarını hızlandırabilir. ne işe yaradığını görmek için. Amaç, hükümet politikası tarafından aranan genel aşılama etkisine katkıda bulunacak sinyaller göndermek olacaktır. Günümüzün zorluklarının önemli bir kaynağı, halkın gördüklerinin doğru olup olmadığına dair bir fikir edinmek için güvenebileceği saygın, güvenilir aracı kaynakların azalmasıdır. Temel doğrulama kuruluşlarının yanı sıra, bu tür gözden geçirilmiş aracı kurumların farklı çeşitlerini denemek, sanal toplumsal saldırganlığın etkisini hafifletmeye yardımcı olabilir.
- *Sanal toplumsal saldırganlığın kullanımını kısıtlayan uluslararası normlar için çalışmaya başlayın* . Sanal toplumsal savaşın en büyük riski, 1945'ten beri büyük ölçüde hüküm süren ve ülkeler arasında barışın korunmasına yardımcı olan toprak bütünlüğü normunun sinsi, kademeli bir bozulmasını temsil etmesi olabilir. Uluslar birbirlerine sanal ama son derece zarar verici şekillerde saldırmaya başladıkları ölçüde, bölgesel saldırmazlık konusundaki yaygın fikir birliği çökebilir ve sonunda büyük ölçekli silahlı maceracılığa yol açabilir. Diğer saldırganlık biçimlerinde olduğu gibi, caydırıcılık savunmaya güçlü bir şekilde katkıda bulunabilir, ancak ülkelerin statülerini ve prestijini temel ilkelere saygı göstermelerine yardımcı olan uluslararası normlar da aynı şekilde olabilir.
- *Özellikle yapay zeka güdümlü bilgi kanalları, sanal ve artırılmış gerçeklik ve algoritmik karar alma gibi gelişen teknolojilerin işleyişini ve güvenlik açıklarını daha iyi anlayın* . ABD ve diğer demokrasiler dikkatli olmazsa, Bu teknolojilerin özel uygulamasındaki ilerlemeler, yoğun güvenlik açıkları yaratarak, politika ve hatta anlayışın önüne geçecektir.

Demokratik toplumlar için yetenekler. Sanal toplumsal savaşın tehlikeleri ve demokratik toplumların ve gelişmiş ekonomilerin bu tür bilgi uygulamalarına özel olarak artan bağımlılığı, bunların potansiyel etkileri ve demokrasilerin kendilerini korumak için atabilecekleri adımlar hakkında araştırma yapılması gerektiğine işaret ediyor.

Bu kategoriler, demokrasilerin potansiyel sanal toplumsal savaş tehdidine karşı kendilerini zırlamaları için gerekli olması muhtemel tepki türünün yalnızca geniş bir taslağını temsil eder. Ortaya çıkan bu saldırganlık biçimleri, daha önce görülmemiş bir ulusal güvenlik tehdidi biçimi olan ileri demokrasiler için önemli bir tehlikeyi temsil ediyor. Özellikle nükleer çağda ve doğrudan bölgesel saldırganlığa karşı genel bir küresel fikir birliğinin hakim olduğu bir çağda, büyük ölçekli istilalar çoğunlukla geçmişte kaldı. Ancak ordular caydırılabilirken, bilgi dünyasının ve ulusların daha geniş sosyal topografyasının kademeli, düşük seviyeli düşmanca manipülasyonu saldırganlığın yeni sınırı olabilir. Sanal toplumsal savaş *potansiyeli* kesinlikle ortaya çıkıyor . Bugün tek soru, demokrasilerin bu tehdide karşı kendilerini kontrol etmek ve savunmak için bir araya gelip gelmedikleridir.

Teşekkür

Yazarlar, projeye verdiği destek ve rehberlik için Net Değerlendirme Ofisine teşekkür eder. RAND Uluslararası Güvenlik ve Savunma Politikaları Merkezi yönetimine -Seth Jones (projenin başlangıcı için), Christine Wormuth (son aşamaları için), Mike McNerney ve Rich Girven'e yönetimdeki yardımları için en içten teşekkürlerimizi sunarız. proje ve raporların geliştirilmesi. RAND'dan Miriam Matthews'a ve Dış İlişkiler Konseyi'nden Adam Segal'e çok faydalı incelemeleri için resmi hakemlere teşekkür ederiz. Yazarlar ayrıca Tim Hwang ve Philip Smith'ten daha önceki taslaklar hakkında gayri resmi yorumlar aldı ve yardımları için çok minnettarız.

Kısaltmalar

yapay	zeka
AR	artırılmış gerçeklik
CGI	bilgisayar tarafından oluşturulan görüntüler
EVM	Eulerian Video Büyütme
GAN	üretken rakip ağı
GPS	Küresel Konumlandırma Sistemi
HD	yüksek çözünürlüklü
IIWAM	bilgisi/etki savaşı ve manipülasyonu
Nesnelerin	İnterneti
NATO	Kuzey Atlantik Antlaşması Örgütü
PFR	yaygın yüz tanıma
POPE'un	pasif seçim ilkesi
TSSB	travma sonrası stres bozukluğu
RFID	radio frekansı tanımlama
VR	sanal gerçeklik

Yeni Bir Çatışma Biçimi

düşmanca sosyal manipülasyon olarak adlandırılabilen bir fenomene ilgi patlaması yaşandı . Artan bu meydan okumaya örnek olarak, Rusya'nın propaganda ve dezenformasyon yoluyla seçimleri etkileme ve Batı'da anlaşmazlık yaratma çabaları; Facebook gibi sosyal medya platformlarının bu tür yanlış bilgilerin yayılmasındaki rolü; ve bölgesel anlatıları şekillendirmek ve belirli ülkelerde siyasi güç kazanmak için gelişen Çin programları. 1 Kongre üyeleri ve üst düzey ABD yetkililerinin yanı sıra alandaki uzmanlar, bu tür taktiklerin ABD demokrasisi ve Avrupa toplumlarının istikrarı üzerindeki zararlı etkileri konusunda giderek daha fazla uyarıda bulunuyorlar.

Bu projenin bir parçası olarak, düşmanca sosyal manipülasyonun zorluğunu tanımladık ve özellikle Rusya ve Çin'in bu alandaki faaliyetlerini izledik. Kavramı , *hedef bir ülkede inançları, tutumları ve davranışları etkileyerek zararlı sosyal, politik ve ekonomik sonuçlar üretmek için amaçlı, sistematik bilgi üretimi ve yayılımı* olarak tanımlıyoruz . Bu raporla, çalışmanın odağını gelecek. Sosyal manipülasyonun arkasındaki teknolojiler ve teknikler için potansiyel gelecek senaryolarını inceliyoruz ve bunların demokrasi üzerindeki olası etkileri hakkında bazı ilk düşünceler sunuyoruz.

Araştırmamız, sosyal manipülasyon çabalarının halihazırda önemli olduğu kadar, Amerika Birleşik Devletleri ve diğer demokrasilerin, bu yaklaşımların bir gün başarabileceklerine dair buzdüğünün yalnızca görünen ucunu gördüğünü gösteriyor. Ortaya çıkan çoklu keşişim

1 Nicholas Thompson ve Fred Vogelstein, "Facebook's Two Years of Hell," *Wired* , Mart 2018.

teknolojiler (belirli bireyler, sanal ve artırılmış gerçeklik, üretilmiş video ve ses ve diğerleri hakkında geniş bilgi veritabanlarına dayanan hedefli pazarlama), saldırganların insanların temel sosyal gerçekliğini değiştirme potansiyelini giderek daha fazla yaratıyor. Bu riskler, bilgi *dünyasının değişen doğası* veya post-modern demokrasileri yöneten bilgi ortamı nedeniyle bugün özellikle önemlidir. Bilgi dünyası, diğer eğilimlerin yanı sıra, otoritenin parçalanması, inanç silolarının yükselişi ve amorf bir sosyal muhalefet adına alaycı ve saldırgan tacizin sürekli “trolling” etiği ile karakterize edilir.

Bugün sürmekte olan tüm eğilimleri doğrusal bir anlamda yansıtmak yanlış olur ve bu analiz bunu yapmamıştır. Bu eğilimlere -sadece iki örnek verecek olursak, giderek daha fazla öne çıkan teyit kuruluşları ve sosyal medya platformlarının bilgi gönderirken güvenilirlik önlemlerini vurgulama talebi şeklinde- bir tepkinin halihazırda başlamış olduğuna inanmak için sebep var. Ancak bu raporun netleştireceği gibi, bilgi dünyasındaki önde gelen eğilimlerin çoğu endişe vericidir ve ortaya çıkan teknolojilerin potansiyel etkileri çok tehlikelidir. Henüz tam olarak anlaşılmayan şekillerde, gelişmiş toplumlar, savunmasız bilgi ve veri toplama, değiş tokuş, iletişim, analiz ve karar verme ağlarına tehlikeli bir şekilde bağımlı hale geliyor.

Gelişmiş algoritmalar, alışveriş kalıpları ve insan sağlığından kişilik faktörlerine ve işe alımlara kadar birçok konudaki verileri giderek daha fazla değerlendiriyor, insanların yaşamları için kritik sonuçları olan tahminler ve kararlar alıyor. Ortaya çıkan Nesnelerin İnterneti (IoT), on yıl içinde bir trilyondan fazla bağlı cihaza sahip olacak - akıllı evler, arabalar, fabrikalar, giyilebilir sensörler ve birbirleriyle iletişim kuran ve günün çoğuna rehberlik eden diğer birçok veri toplama biçimi. -gelişmiş toplumların günlük işleyişi. Pek çok insan, video oyunları, eğlence seçenekleri, iş ve sosyal medyada, sanal gerçeklik (VR) veya artırılmış gerçeklik (AR) cihazları aracılığıyla dünyayla etkileşime girecek ve bu sayede "istedikleri" dünyanın karakterini değiştirebilecekler. görmek için.

Yapay zeka (AI) yetenekleri, tüm bu uygulamalara entegre edilecek ve insan olmayan sistemlerin büyük veri kümelerini giderek daha fazla işlemesine ve anlamasına ve önermesine veya yapmasına olanak tanıyacak.

kilit kararlar. AI güdümlü "oyuncular" dama, satranç, Go ve pokerde en üst sıradaki insan oyuncuları çoktan yendi. AI karar vericilerinin hastalık teşhisinin önemli bileşenlerini veya büyük şirketlerde personel işe alınmasını devralması yalnızca bir zaman meselesidir.

On yıllardır sosyal bilimciler, ileri demokrasilerin endüstriyel bir çağdan *bilgi ekonomisine geçtiğini* , daha çok bilgi üretimi ve alışverişine dayalı olduğunu savundular. fiziksel mallardan daha fazla. ² Bilgi dünyasındaki son değişimler ve gelişmekte olan teknolojilerdeki eğilimler, bu daha büyük geçişin aslında daha yeni başladığını ve biz bunun etkilerini daha yeni görmeye başladığımızı açıkça ortaya koyuyor. Sağlık, ekonomik eşitlik, işe alma, tüketici davranışı ve daha pek çok konuda temel günlük seçimlerin şekillendirildiği ve bazı durumlarda otomatikleştirilmiş bilgi sistemleri tarafından belirlendiği çok daha bilgi merkezli toplumların ortaya çıkışı. işleme—bu geçişin sonuçlarını ve insanların yaşamları üzerindeki etkisini turbo şarj edecek.

Gelişmiş ekonomilerin vatandaşlarına zaten bir bilgi toplumunda yaşadığımızı hissettirse de, aslında bu dönüşümün sadece ilk aşamalarını gördük. Ve bu geçiş, devlet ya da devlet dışı düşman rakiplerine bu toplumlara ulaşmak ve aksamalara, gecikmelere, verimsizliğe ve aktif zarara neden olmak için benzeri görülmemiş fırsatlar sunacak. Ülkeleri nesiller boyu olduğundan daha kalıcı bir şekilde savunmasız hale getirecek sanal toplumsal saldırganlığa kapı açma riskini taşıyor. Bu süreçte, bu tür sanal saldırganlık, ulusal güvenliğin karakterini ve onu korumak için atılan adımları yeniden düşünmeye zorlayabilir.

Bilgi güvenliği uzmanı Bruce Schneier, gelişmekte olan bilgi dünyasının güvenlik açıkları ve özellikle yazılım güvenlik açığı, milyarlarca cihazın karmaşık ağlara bağlı olduğu ortaya çıkan bir IoT ve gelişmiş algoritmaların evliliği ile ilgili en acil uyarılardan bazılarını yayınladı. toplum adına karmaşık kararlar almak. Milyarlarca şey, milyarlarca şey bilgisayara sahip hale geldikçe, risklerin “felaket haline geldiğini” savunuyor.

² Klasik anlatılardan biri Manuel Castells, *The Rise of the Network Society* , New York: Wiley-Blackwell, 2009.

buzdolapları, arabalar, evler, mahkum cezalandırma sistemleri ve tıbbi teşhis süreçleri dahil. ³

Bu rapor, bir merkez RAND analizinin konusu olan Hakikat Bozulması olarak bilinen bir olgunun daha geniş bağlamını araştırmak için yapılan diğer RAND çalışmalarına katılıyor. Bu rapor, *Hakikat Bozulmasını* , aşağıdaki dört bileşenle karakterize edilen, Amerikan yaşamında gerçeklerin ve analizlerin azalan rolü olarak tanımladı:

- Gerçekler ve gerçeklerin ve verilerin analitik yorumları hakkında artan anlaşmazlık
- görüş ve gerçek arasındaki çizginin bulanıklaşması
- Artan göreceli hacim ve sonuçta ortaya çıkan etki, gerçekler üzerindeki görüş ve kişisel deneyim
- daha önce saygı duyulan olgusal bilgi kaynaklarına olan güvenin azalması. ⁴

Bu çalışmanın bakış açısından, bu çalışmada tanımlandığı şekliyle Hakikat Bozulması, daha geniş bilgi küresindeki önde gelen eğilimlerden birini - postmodern demokrasileri düşmanca sosyal manipülasyona karşı savunmasız hale getiren eğilimlerden birini oluşturur. Bu güvenlik açığı kritik bir ilişkiyi vurgular: Agresif sosyal manipülasyon teknikleri, demokrasilerdeki sosyal ve enformasyonel eğilimler üzerine kuruludur ve bunlardan yararlanır - ancak genellikle *yaratamazlar* -. Bilgi dünyasındaki Hakikat Çürümesi ve buna bağlı eğilimler ile eşitsizliğin artması ve seçkinlere olan inancın azalması gibi paralel toplumsal eğilimler temel sorundur. Düşmanca sosyal manipülasyon, devlet veya devlet dışı aktörler tarafından demokrasilere zarar vermek için kullanılan bir tekniktir ve toplumun ve bilginin değişen karakteri üzerinde oynar.

Sosyal manipülasyon peşinde koşarken, saldırganların bir dizi amacı olabilir. Hedef ülkelerdeki tutumları değiştirmeye çalışabilirler - ancak, sosyal bilimlerin üzerine literatür taramasının bulduğu gibi-

³ Bruce Schneier, *Herkesi Öldürmek İçin Buraya Tıklayın: Hiper Bağlantılı Bir Sistemde Güvenlik ve Hayatta Kalma Dünyası* , New York: WW Norton, 2018, s. 78.

⁴ Jennifer Kavanagh ve Michael D. Rich, *Truth Decay: Bir İlk Keşif Amerikan Kamu Hayatında Gerçeklerin ve Analizlerin Azalan Rolü* , Santa Monica, Kaliforniya: RAND Corporation, RR-2314-RC, 2018, s. x-xi.

Öneriler, zorunlu tutum değişikliğinin, bu tür herhangi bir stratejinin en zorlu hedeflerinden biri olduğunu ileri sürecektir. Mevcut tutumları alıp onları yelpazenin daha uç noktalarına doğru itmeye çalışabilirler veya aşırı görüşlere sahip grupları normalleştirmeye ve desteklemeye çalışabilirler. Sosyal medya gönderileri, başka türlü gerçekleşmeyecek gerçek protestolar veya mitingler üretmeyi başardığında olduğu gibi, mevcut dürtüleri harekete geçirmeye çalışabilirler. Süreçte ekonomik maliyetler yükleyerek, bilgi tabanlı bir ekonominin faaliyetlerini ve etkinliğini bozmaya çalışabilirler.

Elbette, sosyal manipülasyon ve sonuçlar -inançlar veya davranış- arasındaki nedensel bağlantı her zaman düz veya doğrusal değildir. Bir toplumun tutum, inanç ve davranış kalıplarının temeli, kolay ve doğrudan manipülasyona tabi değildir. Tutumları değiştirmek zordur ve araştırmalar tutumlar ve davranış arasındaki bağlantının zayıf olabileceğini düşündürmektedir.⁵ Diğer araştırmamız, manipülasyon kampanyalarının bazen tweet veya gönderi sayısı gibi önemli ölçülebilir çıktılar üretebilmesine rağmen, tutum veya davranışlardaki değişiklikler gibi gerçek sonuçları bulmanın çok daha zor olduğunu gösteriyor. Hedef ülkedeki sosyal manipülasyon programları ile sonuçları arasında basit bir ilişki yoktur.

Tanımlar ve Kavramlar

Bu çalışmada, bir toplumda bilgi üretimi, yayılması ve algılanmasının devam eden sosyal sürecine atıfta bulunmak için *bilgiküre terimini kullanıyoruz*.⁶ Bir toplumun bilgi dünyası, en basit haliyle, onun bilgi ortamıdır.

5 Örneğin bkz. Joshua J. Guyer ve Leandre R. Fabrigar, "Attitudes and Behavior", James Wright, ed., *International Encyclopedia of the Social & Behavioral Sciences*, Cilt. II, 2. baskı, New York: Elsevier, 2015.

6 Benzer bir tanım için, bkz. John Arquilla ve David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica, Calif.: RAND Corporation, MR-1033-OSD, 1999, s. 11-12, 16-17. ABD Savunma Bakanlığı'nın "bilgi ortamı" tanımı için bkz. ABD Savunma Bakanlığı, *Ortak Yayın 1-02: Savunma Bakanlığı Askeri ve İlişkili Terimler Sözlüğü*, Washington, DC, Kasım 2010.

kıyafet. Konsept, yayın ve basılı medyayı; sosyal medya; hükümet mesajları ve propagandası; internet ve taşıdığı tüm iletişim ve yayın ağları; bu çıkışları besleyen tüm bilgi üretim kanalları; ve bireylerin bilgi ile etkileşime girme yolları. Düşmanca sosyal manipülasyon kampanyalarının ortaya çıktığı alandır.

Bilgi şekillendirme ve manipülasyon sorununa ilişkin son diyaloglar, neler olup bittiğini açıklamak için bir terim kargaşası kullandı: yanlış bilgilendirme, dezenformasyon, Hakikat Bozulması, propaganda ve diğerleri. Bu çalışma için, düşman aktörlerin ABD'ye veya diğer demokrasilere zarar vermek için bilgi kanallarını kullanmaya yönelik kasıtlı çabalarına atıfta bulunmak üzere tasarlanmış bir terim seçtik. Bu nedenle başlangıçta, inançları, tutumları ve davranışları etkileyerek hedef bir ülkede zararlı sosyal, politik ve ekonomik sonuçlar üretmek için bilginin amaçlı, sistematik olarak üretilmesi ve yayılması olarak tanımladığımız *düşmanca sosyal manipülasyon* terimini kullandık. (Bu terim ve yakından ilişkili diğer terimler, sayfa 7'deki kutuda tanımlanmıştır.)

Kritik bir ayırt edici faktör, düşmanca sosyal manipülasyonun fiziksel varlıkları veya askeri güçleri değil, inançları ve tutumları hedef almasıdır. Bununla birlikte, bu tür manipülasyonun amacı saldırgandır: Düşmanca sosyal manipülasyonun kullanıcısı, hedef duruma zarar vermeye veya bilgi kampanyasını saldırgan, düşmanca eylemler gerçekleştirmesine izin vermek için kullanmaya çalışır.

Yapılması gereken bir ayırım, düşmanca sosyal manipülasyon ile genellikle klasik siber saldırılar olarak anlaşılan şeyler arasındadır. Aslında, siber tekniklerin mümkün kıldığı düşmanca sosyal manipülasyonların çoğuyla, ikisi arasında önemli bir örtüşme var. 7 Ne zaman bir

7 *bilgi/etki savaşı* kavramına ruhen çok yakındır ve Herbert Lin ve Jackie Kerr tarafından sunulan *manipülasyon* (IIWAM). IIWAM'ı şu şekilde tanımlıyorlar: “Bir tarafın düşman hakkında kafa karıştırmak, yanlış yönlendirmek ve nihayetinde rakibin yaptığı seçimleri ve kararları etkilemek için kasıtlı olarak bilgi kullanımı.” Dolayısıyla, hedefleri “düşmanın algıları” olan “düşmanca kinetik olmayan bir faaliyetir”. Bu nedenle, IIWAM konseptleri klasik siber saldırganlıktan farklıdır, çünkü IIWAM alanındaki saldırılar “fiziksel veya dijital eserlerden ziyade “bilgiye, gerçeğe ve güvene zarar vermeye” odaklanır. . . . IIWAM, düşmanın karar verme süreçlerine korku, endişe, belirsizlik ve şüphe aşılamaya çalışır.” Yine de birçok IIWAM saldırısının yapıldığının farkındalar.

Anahtar terimler

- **bilgiküre.** Medya, veri tabanlı algoritmik süreçler ve ağlarda bilgi alışverişi dahil olmak üzere bir toplumda bilgi üretme, yayma ve algılamanın devam eden süreci.
- **Düşmanca sosyal manipülasyon.** Amaçlı, sistematik üretim ve inançları, tutumları ve davranışları etkileyerek hedef bir ülkede zararlı sosyal, politik ve ekonomik sonuçlar üretmek için bilginin yayılması. İnançları, algıları ve gerçekleri manipüle etmeye odaklanma eğilimindedir.
- **Sanal toplumsal savaş.** Düşmanlığın en ayrıntılı veya aşırı biçimi Bu terimi veya kavramı kapsayan ancak bir toplumun bilgi ağlarını bozmak ve manipüle etmek için daha geniş tabanlı bir çabayı ifade eden sosyal manipülasyon. Elektronik ağlardan, algoritmik karar vermeden ve sanal ve artırılmış gerçeklikten elde edilen sonuçları azaltmak veya manipüle etmek için mekanizmalar içerebilir. Konsept, bu tür hedeflere kademeli, kalıcı bir yaklaşımı ifade eder.
- **Siber altyapı saldırısı.** Kötü amaçlı yazılımları veya diğer türlerini kullanma çabaları Önemli fiziksel hasar, bireylere zarar veya sosyal bozulma ve kaos yaratmak için büyük ekonomik veya sosyal altyapıya katastrofik hasara neden olan siber saldırganlık.

Saldırgan, bir taciz kampanyasının veya propaganda çabasının temeli haline gelen bilgileri çalmak için hükümet veritabanlarına girer, esasen sosyal manipülasyon çabası olan şeyi beslemek için siber araçlar kullanır. Yıkıcı tweet'leri yaymak veya Facebook'ta uydurma bilgiler yayınlamak için otomatik botların kullanılması da bu tür amaçlar için bilgi manipülasyon araçlarını kullanır. O halde, iki kategori arasındaki temel ayrım, araçlarda değil, amaçlardadır: Saldırgan, enerji veya su altyapısı gibi şeylere fiziksel zarar vermek için siber araçlar kullandığında, saldırının tutumlar üzerinde etkileri olacaktır, ancak bu etkiler asıl amacı değildir. Bu tür klasik siber saldırılar, düşmanca sosyal manipülasyon dediğimiz şeyin sınırlarının dışında olacaktır. 8

şu veya bu tür siber saldırılarla mümkündür ve bu nedenle “siber etkin IWAM” terimini de kullanırlar. Bkz. Herbert Lin ve Jackie Kerr, *Siber Etkinleştirilmiş Bilgi/Etki Üzerine Warfare and Manipulation*, çalışma kağıdı, Stanford, California: Stanford Uluslararası Güvenlik ve İşbirliği Merkezi, 13 Ağustos 2017, s. 5–7.

8 Bilgi güvenliğine yönelik saldırılar çok çeşitli amaçlar için kullanılabilir, ancak büyük bir ulusal güvenlik odağı, bir toplumdaki kritik altyapıya sızmak, bozmak ve potansiyel olarak ciddi hasara neden olmak için siber araçların kullanımına odaklanmıştır. Bu risklerin bir tedavisi için bkz. Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Bunu Yap*, New York: Ecco, 2010.

Gelişen teknolojiler onları daha da bulanıklaştırmaya çalıştıkça, bu sınırları çizmek daha da zorlaşıyor. Bu zorluk, gelişmiş demokrasilerde karar alma dahil olmak üzere çoğu ekonomik ve sosyal faaliyetin giderek artan bir şekilde temeli olarak hizmet eden bilgi dünyasından kaynaklanmaktadır. Algoritmalar, örneğin hastalık riski, hastalıklar için doğru tedavi, optimal finansal yatırımlar ve hatta suçlar için uygun cezalar hakkında önemli kararlar ve seçimler yapmak için giderek daha fazla kullanılmaktadır. IoT, "akıllı" arabaları, aletleri, saatleri ve daha fazlasını giderek daha fazla veri paylaşan ve ihtiyaçları öngören etkileşimli bir ağa bağlamaktadır.

Bu araştırmanın birincil bulgusu, bu tür eğilimlerin bir sonucu olarak, bir toplumun bilgi dünyasını manipüle etmenin anlamının değişmesidir. Bilgiye dayalı sosyal manipülasyonun geleneksel biçimleri, inançları etkilemek için propaganda, kamu diplomasisi, sosyal medya gönderileri vb. yoluyla anlatıları yaymaya odaklanmıştır. Klasik düşmanca siber saldırılar, bankalar, elektrik santralleri veya santrifüjler gibi fiziksel hedeflere saldırmak için genellikle bilgi ağlarını bir otoyol olarak kullandı. Gelişmiş bilgi kürelerinin evrimi, hızla olası saldırganlığın üçüncü bir kategorisini yaratıyor: Sosyal işleyişin bilgi temellerini manipüle etme veya bozma çabaları. Saldırganlar, giderek artan bir şekilde, yalnızca dezenformasyon ya da olumlu anlatılar yayma ya da fiziksel altyapıya zarar verme değil, aynı zamanda modern toplumların tamamen bağımlı olacağı büyük veritabanlarının, algoritmaların ve ağların işleyişini çarpıtma ve zarar verme fırsatına sahip olacaklar. Bu eylemler, yukarıda tanımlanan sanal toplumsal savaşla ilgili kavram veya kategoriye ana hatlarıyla belirtir ve bu çalışmanın birincil odak noktasıdır - sosyal manipülasyon olarak anlaşılan şeyin çok ötesine geçen, ancak bunun ötesine geçen bir bilgi tabanlı saldırganlık biçimi.

Bu eğilimler, çeşitli bilgi saldırganlığı biçimleri arasındaki ayrımı giderek ortadan kaldırıyor. Bir saldırgan binlerce hastanede kanseri teşhis etmek için kullanılan algoritmayı değiştirebilirse, tedaviyi bozabilir ve bir ülkedeki tıp kurumlarına olan inancı azaltabilir (ve belki de bazı hastaların erken ölümüne katkıda bulunabilir). Akıllı buzdolapları tarafından gıda mağazalarına gönderilen bilgileri ustaca değiştirebilirse, müşteriler tarafında hayal kırıklığı ve belki de gıda israfı ve dolayısıyla ekonomik verimsizlik yaratabilir.

Bu örnekler, nihai olarak fiziksel faaliyetleri kesintiye uğratmak için hala bilgi kanallarının kullanımını içeriyor ve bu nedenle dezenformasyondan ziyade siber saldırılar olarak anladığımız şeye belki de daha yakın. Ancak çoğu durumda bir saldırganın birincil hedefi, fiziksel zarardan çok, kafa karışıklığı ve büyük sosyal kurumların işleyişinde hızlanan güven kaybı olabilir. Nihayetinde, tüm savaşlarda olduğu gibi, hedef düşmanın *iradesidir* ; fiziksel hedeflere yönelik saldırılar sadece bu amaca yönelik bir araçtır. Ve bilgiye bağımlı toplumların ortaya çıkması, saldırganların kullanabileceği sosyal manipülasyon tekniklerinin yelpazesini genişletecek ve derinleştirecek, bu da onların son derece uyarlanmış fiziksel hasar ve tutum değişiklikleri kombinasyonları aramasına izin verecektir. Doğrudan ve yıkıcı fiziksel saldırıların (yukarıda tanımlanan siber altyapı kategorisi) misilleme başlatma olasılığı daha yüksek olduğundan ve büyük ödül düşmanın inançları olduğundan, çoğunlukla, önceliğin tutumsal etkiler üzerinde olacağını görüyoruz.

Neal Pollard, Adam Segal ve Matthew Devost aynı ayrım üzerine yazdılar ve düşmanca sosyal manipülasyonun amacı için kritik bir temayı vurguladılar: güven. Siber saldırılarla ilgili klasik endişeler, aşırı fiziksel hasara neden olma çabalarının “‘bayt ve kan' senaryosu” olarak adlandırdıkları şeye odaklandı. Bu risk ciddi olsa da, genel olarak “siyasi, sosyal ve ekonomik sistemlerin bütünlüğünü yıkmayı” amaçlayan “şimdiye kadar siber çatışma farklı bir yol aldı” yazıyorlar ve “kurumlara olan güveni baltalamak için” diyorlar. manipülasyon, çarpıtma ve bozulma.” Bu tür saldırılar “çok daha düşük bir eşiğe sahiptir, tespit edilmesi ve caydırılması daha zordur ve birbirine bağlı sistemler arasında kademeli olarak ilerleyebilir.” 9

Bu kademeli, kalıcı bir saldırganlık biçimi kavramı, sanal toplumsal saldırganlık kavramının merkezinde yer alır. Saldırganlar bu tür teknikleri kullanarak bir saldırıyı gizleyebilir ve ölçeklendirerek kasıtlı bir şey olup olmadığını belirsiz hale getirebilir. Kurban için, son derece karmaşık sistemlerdeki doğal kusurlar ve verimsizlikler gibi görünecektir. Ancak bunun etkisi hem hedef devletin etkinliğini (ve belki de ekonomik performansını) düşürmek hem de büyük kurumlara olan inancı daha da azaltmak olacaktır.

9 Neal A. Pollard, Adam Segal ve Matthew G. Devost, “Trust War: Dangerous Trends in Cyber Conflict,” *War on the Rocks* , 16 Ocak 2018.

tion. Gerçekten de güvenin rolü bu analizde tutarlı bir temadır. Sosyolog Anthony Giddens ve diğer bilim adamlarının ileri sürdüğü gibi, devasa, son derece karmaşık, teknolojiye bağımlı toplumların zaten bir güven sorunu var: Vatandaşlarından, güvenlik ve refahları için, işleyişini anlamadıkları ve kontrol edemeyecekleri teknolojik ağılara güvenmelerini talep ediyorlar.¹⁰ Bilgi sistemlerinin etkin çalışmasına yönelik saldırılar, doğrudan bu güvenlik açığına saldırır, bu güvenlik açığının işleyişine güvenilemeyeceği duygusunu yaratır ve altında kalıcı bir güvensizlik ve endişe duygusu yaratır.

O halde bu rapor, analizin odağını propaganda, dezenformasyon, hedefli pazarlama, sosyal medya kampanyaları ve inançları ve anlatıları şekillendirmeye yönelik diğer daha doğrudan ve ayrı çabaların ötesine genişletiyor. Kamuoyunun hükümetleri, toplumları ve kendileri hakkındaki tutumlarını etkilemek için ileri demokrasilerin bağlı olacağı bilgi süreçlerinin işleyişini bozmaya ve çarpıtmaya yönelik çabaları içeriyoruz. Konsept, bu tür çabaların birden fazla bilgi aracını kapsayan geniş tabanlı kampanyaları temsil ettiği fikrini içerir; bu, birlikte geçici ve konuya özgü olmaktan ziyade koordineli ve sistematik bir çaba anlamına gelir.

Sadece devletler değil, birçok farklı aktör bu teknikleri kullanabilir. Birçok bilgi manipülasyon tekniğinin azalan maliyeti, ölçeklenebilirliği ve tekrarlanabilirliği ile yapay zeka güdümlü programların saniyeler içinde kötü amaçlı yazılım, bot veya diğer manipülasyon araçları orduları üretme potansiyelinin artması göz önüne alındığında, bu tehdit açıkça devlet dışı aktörleri içerir. Bu analiz, öncelikle tekniklerin yazarlarından ziyade değişen güvenlik açıklarına odaklandı, ancak bu tür araçların yaygın olarak bulunacağını akılda tutmak önemlidir.

Yaklaşım ve Metodoloji

Düşmanca sosyal manipülasyon ve sanal toplumsal savaş gibi karmaşık fenomenlerin geleceğini herhangi bir doğrulukla tahmin etmek imkansızdır.

¹⁰ Örneğin bakınız, Anthony Giddens, *The Consequences of Modernity*, Cambridge, Birleşik Krallık: Polity, 1990.

Bu tekniklerin nasıl gelişebileceğine ışık tutmak için bu analiz iki temel yaklaşımı benimsemiştir. İlk olarak, değerlendirmeyi üç temel konu üzerine ayrıntılı araştırmalara dayandırdık: (1) Amerika Birleşik Devletleri'nde ve diğer ileri demokrasilerde bilgi dünyasının değişen karakterindeki eğilimler; (2) tutumlar ve inançlar üzerine sosyal bilim araştırmalarının içgörüler; ve (3) sosyal manipülasyon uygulamasına dayanan ilgili gelişen teknolojilerdeki gelişmeler. Her üç durumda da, yerleşik araştırma bulguları ve mevcut eğilimler hakkında veri topladık. Ayrıca önümüzdeki beş ila on yıl içinde nasıl oynayacaklarını sorduk.

İkinci Bölüm, ortaya çıkan bilgi küresinin özelliklerine, yani sosyal manipülasyonun oynayacağı bilgi ortamının doğasına ve bu tür tekniklerin geleceği üzerindeki etkilerine ilişkin analizimizi sunmaktadır. Üçüncü Bölüm, en etkili olabilecek sosyal manipülasyon biçimleri hakkında inanç ve tutumlara ilişkin hangi araştırmaların önerdiğini inceleyerek sosyal bilimlerden içgörüler elde eder. Dördüncü Bölüm, gelecekteki manipülasyon kampanyalarında rol oynayabilecek AI'dan VR'ye ve IoT'ye kadar çeşitli teknolojilerdeki mevcut gelişmeleri incelemektedir.

Bu analizde benimsenen ikinci temel yaklaşım, sosyal manipülasyon geleceklerinin olası şeklini tanımlamak için bir senaryo planlama metodolojisi kullanmaktır. Beşinci Bölümden Yedinci Bölüme kadar, eğilimler ve gerçekler üzerine araştırmanın bulgularına, Rus ve Çin sosyal manipülasyon stratejilerine ilişkin paralel çalışmanın içgörülerine dayanarak, sosyal manipülasyonun önümüzdeki on yılda gelişmiş toplumları nasıl etkileyebileceğine dair üç senaryo taslağını çiziyoruz. ve diğer araştırmalar. Üçü birbirini dışlayan değildir; her biri farklı bir temayı vurgular, ancak üçünün öğelerinin gerçek bir geleceği karakterize etmek için birleşmesi muhtemeldir. Her durumda, senaryoların farklı varsayımlarını desteklemek için kapsamlı araştırmalara atıfta bulunuyoruz ve saldırgan sosyal manipülatörlerin avantaj elde etmek için bu senaryonun özelliklerini nasıl kullanabileceğini açıklıyoruz.

Son olarak, Sekizinci Bölüm, analizden elde edilen genel bulguları ve dersleri sunmaktadır.

Gelişen Bilgi Küresi

Sosyal manipölasyon teknikleri bir boşlukta evrimleşmiyor. Gelişmiş demokrasilerde hızla değişen bir bilgi ekosistemi içinde ortaya çıkıyorlar. Bu bilgi üretimi, paylaşımı ve tüketimi bağlamı, çeşitliliği, kapsamı, parçalanması ve erişimi açısından emsalsizdir. Amerika Birleşik Devletleri'nin uğraşmaya çalıştığı sorun, bu değişen ekosistemle ilgili olduğu kadar, amaçlı manipölasyonla da ilgili olabilir. ¹ Bu bölümde, değişen ekosistemin çeşitli yönlerini kısaca inceleyeceğiz.

Gerçek Bozulma üzerine RAND araştırmasının katalogladığı gibi, ABD tarihinin önceki dönemleri, şaşırtıcı seviyelerde “sarı gazetecilik”, uydurma hikayeler, viral dezenformasyon ve en az bir dünya kadar etkilemiş gibi görünen diğer “bilgi kirliliği” gördü. Nüfusun bugünkü oranı etkileniyor. ² Ancak mevcut bilgi dünyası, büyük ölçüde bilgi ortamıyla ilgili bazı ana eğilimlerin bir sonucu olarak, o önceki dönemlerdeki eşdeğerinden çok farklı olabilir. Aşağıdaki bölümler, araştırmamızda ortaya çıkan birkaç ana eğilimi özetlemektedir. Birlikte, hem önemli yeni güvenlik açıkları hem de kamu inançlarını ve anlayışını iyi ya da kötü şekillendirmek için çok daha büyük bir potansiyele sahip bir bilgi dünyası yaratırlar.

¹ Bu argüman Stephan Lewandowsky, Ullrich KH Ecker ve John Cook, “Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era,” *Journal of Hafıza ve Bilişte Uygulamalı Araştırma*, Cilt. 6, Sayı 4, Aralık 2017.

² Kavanagh ve Rich, 2018, s. 41-78.

Daha Geniş Sosyal Eğilimler

İlk önce, bağlamın belirlenmesine yardımcı olan bilgi dünyasının ötesindeki alanlardaki birkaç eğilimi kısaca araştırdık. Aşağıda açıklanan ortaya çıkan bilgi küresinin özellikleri, Amerika Birleşik Devletleri'nin ve Batı'nın çoğunun toplum ve siyasetindeki daha geniş birkaç eğilimle etkileşime girer ve birçok yönden bu eğilimler tarafından daha da şiddetlenir. Bu eğilimler, bilgi geliştirme için kritik öneme sahiptir, çünkü sosyal manipülasyon kampanyaları, etkinlikleri için genellikle daha geniş sosyal bağlama dayanır. Sosyal manipülasyon, bir toplumda tek başına nadiren geniş tabanlı algılar yaratabilir. Bununla birlikte, ortaya çıkan sosyal ve tutumsal eğilimleri kendi avantajına çevirebilir.

En kapsamlı ve önemli eğilim , *vatandaşların operasyonlarını anlama veya kontrol etme yeteneklerini zorlayan ve doğal bir güven sorunu oluşturan büyük ölçekli ve erişime sahip sosyal kurumlar* . Giddens, “uzman sistemlerin” rolünü inceledi postmodern toplumlarda, zaten bir otorite parçalanması, artan bir değişim hızı ve bölgesel kimlik duygusunun yayılması ile karakterize edilen durumlarda. Büyük, teknolojik toplumların “bugün içinde yaşadığımız maddi ve sosyal çevrelerin geniş alanlarını organize eden teknik başarı veya profesyonel uzmanlık sistemlerine” ihtiyacı vardır. İnsanların günlük yaşamları için güvenmeleri gereken, ancak üzerinde çok az kontrole sahip oldukları ve hakkında çok az bilgiye sahip oldukları soyut sistemlerdir. ³ Bu tür kurumlar, insanların birlikte çalıştıkları veya etkileşimde bulundukları devasa şirketlerden küresel bilgi ağlarına ve platformlara, devasa devlet bürokrasilerine kadar her şeyi içerebilir. Bu kurumlar, gelişmiş toplumların temeli haline gelen insan ölçeğinin ötesindeki örgütsel yapılardır. Postmodern, teknolojiye son derece bağımlı toplumun doğası, sosyal manipülasyon kampanyaları tarafından oynanabilecek endişe kaynakları yaratır.

³ —Giddens, 1990, s. 27, 83–100.

Bu yabancılaşma biçimi, insanların *eylemlilik duygusuna*, eylemleri ve sonuçları üzerindeki kontrol algılarına saldırır. 4 Michael Specter'ın "inkarcılık" üzerine yaptığı çalışmasında tartıştığı gibi, "hayatımızın kontrolünü teknolojiye, özellikle zar zor anlayacağımız son derece karmaşık teknolojiye bırakıyoruz ve bunu çok hızlı bir şekilde yapıyoruz" şeklinde yükselen bir his var. bu her yıl hızlanıyor gibi görünüyor.” 5 Aşağıda sıralanan diğer gelişmelerin çoğu, bu kapsayıcı eğilimin bir işlevidir: kitlesel, karmaşık, kişisel olmayan sosyal kurumların insanların sosyal otoriteye olan güvenini sarsma eğilimi.

Pek çok akademisyenin iddia ettiği gibi, bu eğilim Giddens ve diğerlerinin *ontolojik güvenlik olarak adlandırdıkları şeye yönelik bir tehdidi temsil ediyor* . Bu, kişinin hayatındaki olayların ve kalıpların istikrarında yansıtıldığı gibi, kişinin kimliğine duyduğu temel güven duygusuna atıfta bulunur. Kişilerarası ilişkilere ve olayların kişinin benlik duygusuyla uyumlu olduğu duygusuna eleştirel olarak bağlıdır. Bazıları, devletlerin istikrarları için vatandaşlarının ontolojik güvenliğine bağlı olduğunu savundu. 6 Bilgiye dayalı saldırganlık, kısmen bu artan kırılganlığa saldırma ve insanların sosyal kurumlara, kişiler arası alışverişlerine ve onları çevreleyen gerçeklerin ve anlatıların istikrar ve güvenilirliğine olan güvenini daha da zayıflatma çabasıdır.

İlgili bir eğilim, *bir rol oynayan kurumlara olan inancın azalmasıdır. genel olarak kabul edilen sosyal gerçekleri sürdürmedeki rolü* . 7 Bu gösterilmiştir, içinde Amerikalıların medyanın kendisine olan inancı açısından kritik bir örnek: 2016'da yapılan bir Gallup anketi, Amerikalıların kitle iletişim araçlarına olan güveninin benzeri görülmemiş bir şekilde düştüğünü ortaya koydu. 8 Ama aynı zamanda daha geniş bir şekilde gösterilmiştir,

4 James W. Moore, “Faillik Duygusu Nedir ve Neden Önemlidir?” *sınırları Psikoloji* , Cilt. 7, Madde 1272, Ağustos 2016.

5 Michael Spectre, *İnkarcılık: Mantıksız Düşünme Bilimsel İlerlemeyi Nasıl Engeller, Zararları Gezen ve Hayatlarımızı Tehdit Ediyor* , New York: Penguin Press, 2009, s. 33.

6 Jennifer Mitzen, “Dünya Siyasetinde Ontolojik Güvenlik: Devlet Kimliği ve Güvenlik İkilemi,” *Avrupa Uluslararası İlişkiler Dergisi*, Cilt. 12, Sayı 3, 2006.

7 Nathaniel Persily, “Demokrasi İnternette Hayatta Kalabilir mi?” *Demokrasi Dergisi* , Cilt. 28, Sayı 2, Nisan 2017, s. 64.

8 Art Swift, “Amerikalıların Kitle İletişim Araçlarına Güveni Yeni Düşük Seviyeye Düşüyor,” *Gallup* , 14 Eylül 2016. Bkz. Kavanagh and Rich, 2018, s. 33–35, 108–109.

Kongre, büyük şirketler, başkanlık, örgütlü çalışma ve tıp kurumu gibi kurumlara “çok fazla” veya “oldukça fazla” güvendiğini ifade eden Amerikalıların sayısı yüzde 20'nin oldukça altına düştü. ⁹

Haber kaynaklarındaki ve diğer bilgilerdeki değişikliklerin bu eğilimlerle bir ilgisi vardır. ABD tarihinin büyük bir bölümünde, önde gelen haber ve içerik kaynaklarının güvenilir olma ve doğru bilgi aktarma konusunda finansal çıkarları olmuştur. Bugün Facebook, Twitter veya HuffPost olsun, haber toplayıcıları ile durum artık böyle değil: En azından yakın zamana kadar, platformlarındaki içerikten sorumlu oldukları fikrini açıkça reddettiler. Bunlar, içerik sağlayıcılar değil, bağlantı toplayıcılarıdır; bu, toplayıcı platformların sitelerinde görünen içerik için yasal sorumluluklarını ortadan kaldıran 1996 tarihli İletişim Ahlakı Yasası'nın 230. Bölümünde yer alan bir ayrımdır. ¹⁰ (Birkaç sosyal medya platformu şimdi bu duruşu değiştiriyor, dezenformasyon ve aşırı görüşlerle mücadele etmek için daha odaklı çabalar gösteriyor, ancak hiçbirisi Bölüm 230'un temel yasal statüsünden vazgeçmeye hazır görünmüyor.) ¹¹ Bu ayırım, finansal teşvikleri değiştiriyor ve platformların kendi başlarına adım atmaları için daha az motivasyon bırakır. Bilgin Cass Sunstein, bu eğilimi “genel çıkar araçlarının” düşüşü olarak ifade ediyor: geniş kapsamlı, genel olarak paylaşılan haber yayınları ve birçok konuyu ve bakış açısını kapsayan gazeteler. ¹²

Önemli sosyal kurumlara olan azalan inanç, üçüncü bir sosyal eğilimin parçasıdır ; *Amerika Birleşik Devletleri'nde sermaye* . ¹³ Robert Putnam, Amitai gibi yazarlar Etzioni ve William Galston, sivil toplumun düşüşünü katalogladılar.

⁹ Bir dizi veri için bkz. Gallup, *In Depth: Topics A to Z: Confidence in Institutions* , 2018.

¹⁰ Amerika Birleşik Devletleri Yasası, Başlık 47, Bölüm 230, Saldırgan Materyalin Özel Engellenmesi ve Taranması için Koruma, 3 Ocak 2012.

¹¹ Jonathan Vanian, "Facebook, Twitter Sahte Haber ve Manipülasyonla Mücadelede Yeni Adımlar Atın", *Fortune* , 20 Ocak 2018.

¹² Cass R. Sunstein, *#Cumhuriyet: Sosyal Medya Çağında Bölünmüş Demokrasi* , Princeton, NJ: Princeton University Press, 2017, s. 20.

¹³ Lewandowsky, Ecker ve Cook, 2017, s. 357.

tavsiye ve kamu sosyal sermayesinin diğer önlemleri. ¹⁴ Çevre sağlığı ve sosyal güvenlik ağı garantileri gibi ortak refah hedeflerine yönelik kamu taahhüdü gibi, sosyal güven ölçüleri de bir süredir düşmektedir. Bu eğilim, paylaşılan bir bilgi küresinin paralel parçalanması ve karşılıklı olarak şüpheli yankı odalarının yükselişi ile yakından bağlantılıdır.

Dördüncü bir eğilim, Amerika Birleşik Devletleri'nde (ve aslında Batı dünyasının çoğunda) *partizan kutuplaşmasındaki artıştır*. Bu tür partizan önyargı, sosyal bilimin öngöreceği tüm nedenlerle, insanların bilgiyi görme biçimini güçlü bir şekilde şekillendirir. Bilgiye dayalı saldırganlığın sosyal bölünmeler üzerindeki etkisi, kutuplaşmış bir bağlamda, daha partizan olmayan bir bağlamda olacağından daha fazladır. ¹⁵ Bu eğilim artık iyi bir şekilde belgelenmiştir, ancak sosyal medyayla - ve aslında daha geniş bilgi bağlamıyla - ilişkisi bir şekilde belirsizliğini korumaktadır. Levi Boxell, Matthew Gentzkow ve Jesse Shapiro'nun belgelediği gibi, kutuplaşma, sosyal medyayla yoğun bir şekilde meşgul olma olasılığı daha düşük olan yaşlı Amerikalılar arasında da aynı derecede büyük ve genellikle daha fazladır. Polarizasyon, sosyal medyanın ortaya çıkmasından önce zaten yükselişeydi. ¹⁶ Partizan kablolu haberler ve ekonomik durum gibi alternatif faktörler, büyümesiyle sosyal medya kampanyalarından daha yakından ilişkili olabilir. ¹⁷ Bununla birlikte, bir kez kurulduktan sonra, bu tür bir kutuplaşma, sosyal manipülasyon için verimli bir zemin sağlar.

Beşincisi ve kısmen diğer eğilimlerin bir ürünü olarak Batı, birçok gelişmiş ülkenin ekonomik ve kültürel koşullarından duyulan derin memnuniyetsizliği yansıtan *popülist hareketlerin yükselişine tanık oldu*.

¹⁴ Robert Putnam, *Tek Başına Bowling: Amerikan Topluluğunun Çöküşü ve Canlanması*, New York: Simon ve Schuster, 2001.

¹⁵ Amanda Taub, "Sahte Haberin Gerçek Hikayesi Partizanlıktır," *New York Times*, 11 Ocak 2017.

¹⁶ Levi Boxell, Matthew Gentzkow ve Jesse M. Shapiro, "Daha Fazla İnternet Kullanımı, ABD Demografik Grupları Arasındaki Politik Kutuplaşmanın Daha Hızlı Büyümesiyle İlişkili Değil", *Proceedings of the National Academy of Sciences*, Cilt. 114, No. 40, Ekim 2017a.

¹⁷ Gregory J. Martin ve Ali Yörükoğlu, "Kablo Haberlerinde Önyargı: İkna ve Kutuplaşma," *American Economic Review*, Cilt. 107, No. 9, 2017. Ayrıca bkz. Levi Boxell, Matthew Gentzkow, ve Jesse M. Shapiro, "Medya Amerikalıları Aynı mı Sürükleyiyor?" *New York Times*, 6 Aralık 2017b.

toplumlar. ¹⁸ Bu yaygın fenomen, Avrupa'da hem sağ hem de sol aşırılıkçı partilerin yükselişini ateşledi ve bir süre daha devam edecek gibi görünüyor. ABD ve Avrupa siyasetinin kutuplaşmasını şiddetlendirdi, yeni korumacılık ve yabancı düşmanlığı nöbetleri yazdı ve Batılı siyasi kurumların güvenilirliğini sorguladı.

Bu nedenle, çalkantılı bir siyasi ve sosyoekonomik bağlamda sosyal manipölasyon ve sanal toplumsal saldırganlık kampanyaları gerçekleşiyor. Toplumlara yönelik sanal saldırganlık, toplumlardaki mevcut zafiyetler üzerinde oynayabileceği ölçüde önemli bir etkiye sahiptir. Meslektaşımız Rand Waltzman, “bilişsel kırılmalık” fikrini önerdi ve mevcut bağlam, önemli derecede böyle bir savunmasızlık yaratıyor. ¹⁹ İleri demokrasilerin bilgi kürelerinin değişen karakteri, bu nedenle, bu daha temel toplumsal eğilimleri şiddetlendirmeye (veya hafifletmeye) hizmet edebilir.

Bilgi Dünyasındaki Eğilimler: Bilgi ve Farkındalık

Bu genel sosyal eğilimler enformasyona dayalı saldırganlık için yollar yaratsa bile, bu tür saldırganlık aynı zamanda bilgi küresinin kendi karakterinde ortaya çıkan gerçekliklerden de yararlanabilir. Aşağıdaki bölümler, aşağıdakiler de dahil olmak üzere, bu tür sekiz gerçekliği inceler:

- ağ dinamikleri ve bilginin viral yayılmasının rolü
- haberlerde ve diğer medyada geniş tabanlı sansasyonizm

¹⁸ Batı'daki popülist dalga üzerine çok sayıda kitap ve rapor ve yüzlerce haber hesabı da dahil olmak üzere çok geniş bir literatür var. Kapsamlı değerlendirmeler için bkz. John B. Judis, *The Populist Explosion*, New York: Columbia Global Reports, 2016; ve Jan-Werner Müller, *Popülizm Nedir?* Philadelphia, Pa.: University of Pennsylvania Press, 2016. Bir sınav için popülist dalga için ekonomik ve kültürel argümanlar hakkında bkz. Ronald Inglehart ve Pippa Norris, *Trump, Brexit ve The Rise of Populism: Economic Have-Nots and Cultural Backlash*, fakülte araştırma çalışma kağıdı, Cambridge, Mass.: Harvard Kennedy School, RWP16-026, Ağustos 2016.

¹⁹ Rand Waltzman, “The Weaponization of Information: The Need for Cognitive Security”, Senato Silahlı Kuvvetler Komitesi önünde sunulan ifade, Siber Güvenlik Alt Komitesi, Santa Monica, Kaliforniya: RAND Corporation, CT-473, 27 Nisan 2017, s. . 3.

- bilgi küresinin parçalanması
- bilgi platformlarının yoğunlaşması
- kendini güçlendiren yankı odalarının etkisi
- etkileyicilerin rolü
- internette bir “trolling etiğinin” ortaya çıkışı
- bireyler ve gruplar hakkında veri toplamının patlayıcı büyümesi.

Bazı durumlarda, bilgi küresinin mevcut durumu geçmişten bariz bir şekilde farklı değildir. Ancak bu alanların birçoğundaki gelişmeler – özellikle parçalanma, yankı odaları ve trolling etiği – mevcut ve ortaya çıkan bilgi bağlamını öncekilerden keskin bir şekilde ayıran özelliklere sahiptir.

Bu eğilimler için temel bilgi tabanına bir soru gider: halkın önceki dönemlerde olduğundan daha fazla yanlış bilgilendirilmiş olup olmadığı meselesi. ²⁰ “Ekonomiden dış politikaya kadar pek çok konuda yanlış algılamalar yaygın görünüyor.” ²¹ Bazı araştırmalar, ABD’li üniversite mezunlarının yeterli eleştirel düşünme veya temel bilgi edinmedikleri için sert eleştirilerde bulundu. ²² Örneğin, 1970’lerin sonu ile 1990’ların sonu arasındaki büyük gazetelerin içeriği üzerine yapılan bazı araştırmalar, eğlence, fikir ve sansasyonelliğe artan bir vurgu ve saf gerçeğe daha az odaklanıldığını buldu. Gazete abonelikleri yerini kablolu haber izleyiciliğine bırakıyor ve bu tür ağlardaki pek çok program tartışmayı, tartışmayı ve bazı durumlarda gerçekler üzerinde partizan dönüşü vurguluyor. ²³

Ancak asıl soru, yanlış bilginin eskisinden daha kötü olup olmadığı ve mevcut kanıtların çoğu öyle olmadığını gösteriyor. Bunun yerine,

²⁰ Genel cehalet meselesi için bkz. Jason Brennan, “Trump Won Çünkü Voters Are Ignorant, Literally,” *Foreign Policy* , 10 Kasım 2016; Jared Meyer, “The Ignorant Voter,” *Forbes* , 27 Haziran 2016; ve Andrew Romano, “Amerikalılar Ne Kadar Cahil?” *Haber Haftası* , 20 Mart 2011.

²¹ DJ Flynn, Brendan Nyhan ve Jason Reifler, “Yanlış Algıların Doğası ve Kökenleri: Siyaset Hakkında Yanlış ve Desteklenmeyen İnançları Anlamak,” *Politik Psikoloji* , Cilt. 38, Ek. 1, 2017, s. 129. Bu konuda başka literatürden de alıntı yaparlar.

²² Tom Nichols, “Mezunlarımız Rubes,” *Chronicle of Higher Education* , 15 Ocak 2017a.

²³ Kavanagh ve Rich, 2018, s. 106–107.

Kanıtlar, bir demokraside genel bir kamuoyunun tipik olarak birçok fenomen hakkında birçok yanlış izlenimi sürdürdüğünü gösteriyor. Örneğin bir Pew Araştırma Merkezi araştırması, 1989 ile 2007 arasında, ticaret politikası, üst düzey siyasi liderlerin adları ve Kongre'deki parti dengesi gibi konularda genel kamuoyu farkındalığının çok az değiştiğini ileri sürdü. Bazı konular hafif bir düşüş gösterdi, diğerleri hafif bir artış gösterdi. ²⁴ Çalışma, bilgi dağılımında, halkın “en bilgili üçte birinin” varlığı gibi, diğerlerinden daha fazla bilgi arayan ve daha iyi bilgilendirilmiş olan kalıcı kalıplar buldu. Eğitim, “bilginin en iyi tek tahmindir” olarak kaldı.

Olgusal doğruluğa saygı ortadan kalkmadı; insanlar hala ciddiyete ve uzmanlığa değer veriyor. Birleşik Krallık'ta yapılan bir anket, yanıt verenlerin yüzde 85'inin haber kaynaklarının uzmanlara danışmasını istediğini ortaya koydu. Amerikalıların yaklaşık yüzde 90'ı, gerçekleri doğru anlamının önemli olduğuna inanıyor. ²⁵ "Motive edilmiş akıl yürütme"nin -insanların yerleşik görüşleriyle uyumlu bilgi ve kredi arama eğiliminin- önemli bir etkisini gösteren araştırmalar bile, bir dereceye kadar bir "doğruluk motivasyonu" ile etkisiz hale getirilir. ²⁶

Süreçte, bu eğilimler insanların algılarını ve nihayetinde davranışlarını birkaç farklı düzeyde etkileyebilir. *Tutumlar* terimi yaygın olarak kullanılır, ancak belirli bir yapı türüne atıfta bulunur: insanların fikirler, sorunlar, olaylar ve diğer insanlar gibi şeylere ilişkin değerlendirmeleri. Ancak bilgi küresinin değişen karakteri, sahip oldukları bilgi türü ve uygun gördükleri davranışlar da dahil olmak üzere diğer algı ve anlayış düzeylerini de etkileyebilir. Gerçekten de onlardan biri

²⁴ Pew Araştırma Merkezi, *Halkın Güncel Olaylara İlişkin Bilgisi, Haberler ve Bilgi Devrimleri*, Washington, DC, 15 Nisan 2007, s. 1.

²⁵ Bruce Wharton, Shawn Powers ve Markos Kounalakis, editörler, *Can Public Diplomacy Survive the Internet?* Washington, DC: ABD Kamu Diplomasisi Danışma Komisyonu, 2017, s. 8.

²⁶ Klasik bir tedavi, Ziva Kunda'dır, "Motive Reasoning Case", *Psikolojik Bülten*, Cilt. 108, No. 3, Kasım 1990. Ayrıca bkz. Nicholas Epley ve Thomas Gilovich, Motivated Reasoning'in Mekanığı, *Journal of Economic Perspectives*, Cilt. 30, Sayı 3, 2016; ve David P. Redlawsk, “Hot Cognition veya Cool Düşünce? Motive Edilmiş Akıl Yürütmenin Siyasi Karar Verme Üzerindeki Etkilerinin Test Edilmesi,” *Journal of Politics*, Cilt. 64, Sayı 4, 2002.

Aynı anda pek çok psikolojik alanı etkileyebilecek ve manipölasyonunun bilgiyi, tutumları ve davranışları şekillendirebileceği kapsamlı, derinden gömülü bir bilgi küresinin hem heyecan verici hem de tehlikeli yönleri.

Ancak demokratik halklar tarafından tutulan temel bilgi düzeyi, herhangi bir bilgi küresinin karakterini şekillendiren denklemin yalnızca bir parçasıdır. Aşağıdaki bölümler, ortaya çıkmakta olan bilgi ortamının önde gelen bazı özelliklerini özetlemektedir.

Ağa Bağlı Dinamikler ve Bilginin Viral Yayılımı

Bilgi küresinin merkezi bir bileşeni, giderek daha fazla ağ oluşturan, birbirine bağımlı karakteridir: hem fırsatlar hem de önemli güvenlik açıkları yaratan “birbiriyle ilişkililiğin” temel bir özelliği. ²⁷ Bu ağ bağlantılı kalite, iddiaların ve anlatıların sosyal medya ve diğer kanallardaki yoğun ağlar aracılığıyla hızla yayılması ve ayrıca veri tabanları ve ağların artan birbirine bağlılığı ile bilgi alışverişini içerir. Bu değiş tokuşlar, gelişmekte olan IoT'den, aynı büyük teknoloji firmasına ait çeşitli uygulamalar ve şirketler tarafından toplanan tüketiciler hakkında bilgi veritabanlarına kadar uzanmaktadır.

Bu karşılıklı bağlantının bir anlamı, fikirlerin, bilgilerin veya anlatıların viral yayılma potansiyelidir. "Viralite" sorunu - hangi raporların viral hale geldiğini ve hangilerinin gitmediğini anlamak - hala tam olarak anlaşılmış değil. ²⁸ Birkaç düşündürücü araştırma bulgusu, bilginin "viralleşmesine" yardımcı olan çeşitli özelliklere işaret ediyor, ancak henüz bu tür sonuçları her koşulda öngörebilecek kapsamlı bir teori yok. Araştırmalar, örneğin, bir ağdaki tanımlanabilir etkili kişilerin bilginin yayılmasında orantısız bir rol oynayacağını öne sürdü ve bazı araştırmalar,

²⁷ Bu Albert-László Barabási'nin ana tezidir, *Linked: How Everything Is Connected Diğer Her Şeye ve İş, Bilim ve Günlük Yaşam için Ne Anlama Geldiği*, New York: Temel Kitaplar, 2014, s. 5.

²⁸ Sunstein, 2017, s. 102–103, bilgi akışının nedenlerinin belirsizliğini koruduğunu ve viral hale gelen gerçek paylaşılan bilgilerin (şarkılar gibi) oldukça rastgele olduğunu öne süren vakalara atıfta bulunur.

viral haberlerin yayılma kalıpları ve özellikleri. ²⁹ Bununla birlikte, bunun ötesinde, belirli bir hikayeyi neyin viral hale getirdiği iyi anlaşılmamıştır. Hikayelerin yalnızca küçük bir kısmı bunu yapacak ve görünüşe göre liste önemli düzeyde şans içeren keyfi olacak. ³⁰

Son araştırmalar, hikayelerin viral olma eğiliminde olan bir diğer özelliğine işaret ediyor: Yeni ve büyüleyici olma eğilimindedirler. Uydurma veya abartılı haberler, yayılmalarını artırmak için bu faktöre oynayabilir. Bir çalışmanın yazarları, "Yanlış, çalışmadaki tüm bilgi kategorilerinde gerçeklerden önemli ölçüde daha uzağa, daha hızlı, daha derine ve daha geniş bir şekilde yayıldı" dedi. Bazı durumlarda, 1.500 kişiye ulaşmak için doğru hikayelerin yanlış olanlardan altı kat daha uzun sürdü; yalanların retweet edilme olasılığı, gerçek hikayelere göre yüzde 70 daha fazlaydı. ³¹ Yine de çalışmanın ilginç bir anlamı vardı: Viralitenin bu nitelikleri, otomatik tepkiler için değil, insan tepkileri için geçerlidir. Bot ağları, belki de hikayelerdeki yenilik unsurlarına tepki vermedikleri için, doğru ve yanlış eşit miktarlarda yayma eğilimindeydi.

Bu faktörler, bu fenomenin yadsınamaz bir yönüne işaret eder: Bilginin viral bir şekilde yayılması veya basamaklandırılması, bir fenomendir.

29 Örneğin, bkz. Justin Cheng, Lada Adamic, P. Alex Dow, Jon Michael Kleinberg ve Jure Leskovec, "Cascades Be Predicted?" *Yirmi Üçüncü Uluslararası Dünya Çapında Web Konferansı*, *Konferans Bildirileri*, Seul: Bilgisayar Makineleri Derneği, 2014. Daha geniş bir inceleme için bkz. Lee Daniel Kravetz, *Strange Contagion*, New York: Harper-Collins, 2017, viral yayılmayı tetiklemede sosyal bağlantıların rolünü vurguluyor. Pazarlama profesörü Jonah Berger konuyu inceledi ve viralitenin altı temel özelliğini önerdi: sosyal para birimi (insanların havalı ve bilindik göründükleri için paylaşmak istedikleri gerçekler); tetikleyici uyarılar; duygusal çekiciliklerin kullanımı; popüler ilgi; insanlar için pratik değeri olan gerçekler; ve anlatılara veya hikayelere gömülü gerçekler; Jonah Berger, *Bulaşıcı: Neden Şeyler Yakalanıyor*, New York: Simon ve Schuster, 2013.

30 Örneğin, Twitter'daki viral örüntüler üzerine yapılan büyük bir araştırma, daha etkili kullanıcıların hikayelerin veya hashtag'lerin viral yayılmasıyla daha fazla ilişkili olmasına rağmen, aslında virallüğün nispeten önceden tahmin edilemez bir fenomen olarak kaldığını, yani bilgiyi yaymak için tek etkili stratejinin şu anlama geldiğini buldu. sadece mümkün olduğu kadar çok etkileyiciyi hedeflemek ve en iyisini ummak. Eytan Bakshy, Jake M. Hofman, Winter A. Mason ve Duncan J. Watts, "Everyone's an Influencer: Quantifying Influence on Twitter," *Fourth ACM International Web Arama ve Veri Madenciliği Konferansı*, *Konferans Bildirileri*, Hong Kong: Dernek Bilgisayar Makineleri için, 2011.

31 Soroush Vosoughi, Deb Roy ve Sinan Aral, "The Spread of True and False News Online," *Science*, Cilt. 359, No. 6380, 2018, s. 1146.

sosyal etki. İnsanlar diğer insanların söylediklerini, yaptıklarını ve “beğendiklerini” takip ediyor. Bir hikayenin, memin, gif’in veya şarkının diğerinin aksine viral hale gelmesinin belirli nedenleri gizemli olabilir, ancak temel mekanizma değildir: Bu bir tür sosyal kanıt etkisidir. Bir çıkarım, bu tür kaskadların, özellikle sosyal olarak etkili aktörlerden gelen erken ve önemli onaylarla tetiklenebileceğidir. Her iki durumda da, kaskadlar ya çok hızlı bir şekilde başlayabilir ya da karaya oturabilir, bu da sosyal manipülasyon alanında kritik bir ilk hamle avantajına işaret eder.³²

Sayısallaştırılmış ağlar aracılığıyla yayılabilen tek şey bilgi değildir. 2012’de yaklaşık 700.000 kullanıcıyla yapılan bir Facebook araştırması, “ruh halinin bulaşıcı olduğunu” buldu. Facebook, insanların haber akışlarına giren olumlu ve olumsuz hikayelerin dengesini değiştirerek, ruh hallerini ölçülebilir şekillerde değiştirebildi ve bu insanlardan daha fazla sayıda olumsuz gönderi gibi sonuç davranışları üretebildi. Çalışma, “duygusal durumlar”, “başkalarına aktarılabilir” sonucuna varıyor.³³

sansasyonellik

Haber medyasında ve daha geniş anlamda bilgi dünyasında son otuz yılda önemli bir eğilim, içerik ve habercilik tarzındaki sansasyon derecesinde ölçülebilir bir artış olmuştur. Sansasyonelizmin genel sorunu yeni değil - günümüzün eğilimi, 19. yüzyılın sonundaki kötü şöhretli sarı gazetecilik çağı gibi daha önceki dönemleri yansıtıyor.³⁴ Üstelik, sansasyonelizmin yükselişine dair güçlü bir anekdotsal his olsa da, son on yılda büyümesini ölçmeye çalışan az sayıda çalışma var. Bununla birlikte, bir dizi kaynaktan elde edilen kanıtlar, ana akım ve niş bilgi kaynaklarının, dikkat çekmek için giderek daha fazla sansasyonel hesaplara bel bağladığını göstermektedir.

Büyüyen sansasyonelizmin motorunun bir kısmı, birçok web sitesinin sansasyonel içerik üretmek amacıyla tasarlanmış olmasıdır.

³² Sunstein, 2017, s. 111–114.

³³ Cathy O’Neil, *Weapons of Math Destruction: Büyük Veri Eşitsizliği Nasıl Artırıyor ve Demokrasiyi Tehdit Ediyor*, New York: Broadway Books, 2016, s. 184.

³⁴ Kavanagh ve Rich, 2018, s. 42–50.

sitelerin temel iş modeli olan en fazla sayıda izleyiciyi çekmek. Gawker önde gelen bir örnektir: siyasi aktivist Eli Pariser, içerik oluşturucuların odasının üzerinde gezinen site trafiğinin “Büyük Panosu”nu tanımlar. Gawker yazarları için temel gereksinim, trafik oluşturmak ve Big Board'u yapmaktır; içerik önemsiz değilse de ikincildir. ³⁵ Geleneksel haber medyası bile, okuyucuları ve izleyicileri aşırı içeriğin olduğu bir çağda tutmak için, hikayelerinin biçim ve içeriğinde daha sansasyonel hale geldi. ³⁶

Diğer araştırmalar, YouTube gibi kendi içeriklerini üretmeyen sitelerde bile aşırılık yanlısı önyargı olduğunu öne sürüyor. Oynatma listesi algoritmasının orantısız bir şekilde "kullanıcıları komplo teorileri, partizan bakış açıları ve yanıltıcı videolar içeren kanallara yönlendirdiği" tespit edildi. ³⁷ Bu önyargı, kullanıcıları izlemeye devam etmeye öncelik veren bir algoritmanın sonucu gibi görünüyor ve bu nedenle, sansasyonelizmin bir ürünü olabilecek, yüksek ilgiye sahip önerilecek videoları arayacak.

YouTube sonuçları, virallüğün artık hangi içeriğin önerileceğini belirlemede önemli bir rol oynaması anlamında, bağlantılılıkla ilgili daha büyük bir eğilimi yansıtıyor. ³⁸ Medya kuruluşlarının birincil amacı izleyiciyi sürdürmektir. Bu, başkalarının en çok görüntülediği, paylaştığı veya önerdiği makaleleri zorlamak anlamına gelir ve bunlar genellikle en sansasyonel, dikkat çekici makalelerdir. Sonuç, medya kuruluşlarını daha fazlası yönünde iten, kendi kendini güçlendiren bir süreçtir.

³⁵ Eli Pariser, *Filtre Balonu: İnternet Sizden Ne Saklıyor*, New York: Penguin Press, 2011, s. 69.

³⁶ Bakınız, örneğin, PH Vettehen ve M. Kleemans, “Proving the Obvious? Duyumsalcılığın Haber Videosunda Harcanan Zamana Katkıları Nedir?” *Electronic News*, Cilt. 12, Sayı 2, 2018; ve DK Itssu, *News as Entertainment: The Rise of Global Infotainment*, Londra: SAGE Publications, 2007.

³⁷ Jack Nicas, “YouTube İnsanları İnternetin En Karanlık Köşelerine Nasıl Çekiyor”, *Wall Street Dergi*, 7 Şubat 2018.

³⁸ Bharat N. Anand, “ABD Medyasının Sorunları Sahte Haberlerden ve Filtre Baloncuklarından Çok Daha Büyük,” *Harvard Business Review*, 5 Ocak 2017.

sansasyonel, genellikle aşırı içerik. ³⁹ Bu etkiler özellikle sosyal medyada dikkat çekici olabilir. ⁴⁰

Sansasyonel haberlere yönelik eğilimin bir anlamı, “karamsarlık sendromu” olarak adlandırılan şeydir. ⁴¹ Kısmen, ezici bir çoğunlukla olumsuz olan medya kapsamı tarafından körüklenen - birçok yankı odasının tek taraflı mesajlarıyla daha da şiddetlenen kapsama - birçok insan, önemli sosyal göstergelerin durumunun ve eğilimlerinin (işsizlik gibi konularda) olduğuna inanmaya başladı. , göçmenlik ve suç) durumda olduğundan çok daha kötüdür. Bu haber, genelleştirilmiş bir yanlış bilgi biçimini oluşturur, biri ana eğilimler ve sosyal gerçekler hakkında olumsuz bir görüşe eğilimlidir. Bazı analizler, siyasi haber raporlamasındaki olumsuz önyargının çok önemli olduğunu ve büyük kurumlara olan inancın azalmasına katkıda bulunduğunu ileri sürüyor. ⁴² Sonuçlar, bir kez daha, sosyal manipülasyon stratejileri tarafından kullanılabilecek şikayet ve hayal kırıklığı seviyeleridir.

Bilgi Kaynaklarının Parçalanması

Yayın ve bilgi endüstrileri tarihinde, *The Attention Merchants* , yazar ve profesör Tim Wu, temel bir noktayı vurguluyor. Amerikalılara ulaşan bilgi kaynaklarında parçalanma eğilimi. ⁴³ Bu parçalanma, 1950'ler ve 1970'ler arasında, birkaç televizyon ağının (ve onların içinde, belirli şovların) bilgi dünyasına hakim olduğu, ilginin en üst düzeyde olduğu dönemden kayda değer bir değişikliği yansıtıyor. Wu'nun belgelediği gibi, en baskın şovlar (*I Love Lucy* gibi)

³⁹ Anan, 2017.

⁴⁰ Robert Kozinets, “Sosyal Medya İnsanların Tutkularını Nasıl Ateşliyor—ve Aşırılıkçı Bölümler Oluşturuyor,” *The Conversation*, 13 Kasım 2017.

⁴¹ Michael J. Mazarr, “Karamsarlık Sendromu,” *Washington Quarterly* , Cilt. 21, Sayı 3, 1998.

⁴² Bkz. Tom Stafford, “Psikoloji: Neden Kötü Haber Manşetlere Dominate”, *BBC* , 29 Temmuz 2014.

⁴³ Tim Wu, *The Attention Merchants: The Epic Scramble to Get Our Heads* , New York: Vintage Books, 2016.

izleyenlerin yüzde 70'inden fazlasını aldı ve bazı olağandışı olaylar (Elvis Presley'in *The Ed Sullivan Show*'daki görünümü gibi) yüzde 80'den fazla pay aldı. Hem eğlencede hem de haberlerde, çoğu Amerikalı aynı şeylerin çoğunu izledi. 1970'lerin sonlarında, özellikle Amerika Birleşik Devletleri'nde kırk belirli "alt ulus" yaratan ünlü PRIZM pazarlama modelinde, nüfus arasındaki çeşitlilik "kümeleri" vurgusuyla başlayarak, izleyicilerin parçalanması hızlanarak başladı. İnternet aracılığıyla, düzinelerce kanal ve milyonlarca blog, web sitesi ve sosyal medya beslemesinden oluşan günümüzün inanılmaz çeşitlilikteki yayın ortamına ve beraberindeki küçük niş segmentlerin mikro hedeflemesine yol açar.

Ortaya çıkan parçalanma, tartışmasız mevcut bilgi küresine yansıyan en önemli yapısal değişikliktir. Amerikalılar (ve tüm gelişmiş, açık toplumların vatandaşları) bugün düzinelerce kablolu kanal ve radyo istasyonundan haber, bilgi ve farkındalık almak için esasen sınırsız seçeneklere sahiptir; çevrimiçi varlıkları olan çok çeşitli baskı kaynakları; ve yüzlerce web sitesi, blog ve podcast. Ortaya çıkan kafa karışıklığı, muhtemelen herhangi bir toplumun ortak anlatıları veya kamusal anlayışları sürdürmesini çok daha zor hale getiriyor. Aynı zamanda, bir sonraki bölümde tartışılacak olan yankı odalarını güçlendirerek, insanlara yerleşik inançlarını güçlendirmek için gelen bilgileri uyarlamak için benzeri görülmemiş bir yetenek sağlar.

Zorluk, yalnızca birbiriyle rekabet halindeki haber öykülerini anlamlandırmaktan daha temeldir: Gelişmiş toplumların gelişen doğasıyla ilgilidir. Giddens, "post-modernitenin koşulu, 'büyük anlatı'nın buharlaşmasıyla ayırt edilir - kesin bir geçmişe ve öngörülebilir bir geleceğe sahip varlıklar olarak tarihe yerleştirildiğimiz kapsamlı bir 'hikaye çizgisi'." ⁴⁴ Parçalara ayrılmış bir medya alanında, günlük olaylara tutarlılık kazandıracak büyük bir anlatı yoktur.

Amerikalıların üçte ikisi şimdi anketlerde haberlerinin en azından bir kısmını sosyal medyadan aldıklarını bildiriyor - en önemli son kazanımların ölçüldüğü yaşlı Amerikalılar da dahil. Birden fazla kişiden haber ve bilgi almaya devam ederler.

⁴⁴ Giddens, 1990, s. 2.

kaynaklar: yerel televizyon, kablolu televizyon istasyonları, ağ haberleri, radyo ve (en azından) basılı gazeteler. ⁴⁵ Düzinelerce veya yüzlerce site arasında dağıtılan genel olarak çevrimiçi haber tüketimi, televizyon haberlerini izleme hızına yetişiyor: Ağustos 2017'de yapılan bir ankette, Amerikalıların yüzde 43'ü çevrimiçi "sıklıkla" haber aldıklarını söyledi, bu oran yüzde 50 televizyondan. Fark, sadece bir yıl önce neredeyse yüzde 20'den kapanmıştı ve daralmaya devam edecek gibi görünüyor. Bu çevrimiçi kaynaklar, önemli derecede sosyal medya görüntülemeyi içeriyor: Aynı ankette, Amerikalıların üçte ikisi sosyal medyadan "bazı" haberler aldıklarını bildirdi. ⁴⁶ 2018'de yapılan bir anket, Amerikalıların yüzde 20'sinin sosyal medyadan "sıklıkla" haber aldığını ve yüzde 27'sinin "bazen" aldığını ortaya koydu. ⁴⁷ Sonuç, daha önceki dönemlerin tekdüzeliğinden yoksun karmaşık bir bilgi kaynakları ağıdır.

Bazı araştırmalar, çelişen mesajların karıştırılmasının bir avantajı olduğunu öne sürüyor: Sosyal manipülasyona karşı bir koruma sağlayabilir. ⁴⁸ İnsanlar tek bir bilgi kaynağına maruz kaldıklarında, inançlar üzerinde anlamlı bir etki mümkündür. Ancak tartışmalı gerçekler atmosferinde bu çok daha zor hale gelir. Çok az Amerikalı çevrimiçi kaynaklardan aldıkları haberlere *güveniyor* -yalnızca yüzde 5'i bilgiye "çok" güveniyor ve teoride bu güven eksikliği, bu tür bilgilerin tutumlar üzerindeki kolay etkisine karşı bir filtre sağlamalı. ⁴⁹

Ancak burada bir ikilem olduğu açıktır: Parçalanma, bir manipülatörün tek bir alternatif gerçeklik yaratmasını zorlaştırabilir, ancak aynı zamanda paylaşılan sosyal bilgi ve bilgi kurumlarını da baltalar.

⁴⁵ Elisa Shearer ve Jeffrey Gottfried, "Sosyal Medya Platformlarında Haber Kullanımı 2017," *Pew Araştırma Merkezi*, 7 Eylül 2017.

⁴⁶ Kristen Bialik ve Katerina Eva Matsa, "Sosyal ve Dijital Haber Medyasında Temel Trendler," *Pew Araştırma Merkezi*, 4 Ekim 2017.

⁴⁷ Katarina Eva Matsa ve Elisa Shearer, "News Use Across Social Media Platforms 2018," *Pew Research Center*, 10 Eylül 2018.

⁴⁸ Araştırmalar, "tek kaynaklı" veya tek sorunlu bilgi veya büyük ölçüde eğimli bilgi ortamlarının tutumlar ve davranışlar üzerinde önemli etkileri olabilse de, zemin anlamlı bir şekilde tartışıldığında veya birçok farklı konu arasında bulanıklaştığında bu etkilerin hızla düştüğünü; Anthony R. Pratkanis ve Elliot Aronson, *Age of Propaganda: The Everyday İkna Kullanımı ve Kötüye Kullanımı*, New York: Henry Holt and Company, 2001, s. 29-30, 83-84.

⁴⁹ Bialik ve Matsa, 2017.

bir zamanlar dezenformasyona ve sosyal manipölasyona karşı önde gelen siperi sağlayan farkındalık. Gelecekteki zorluk, büyük ölçüde parçalanmış olarak kalacak bir çevre içinde daha küçük bilgi araçlarından oluşan karmaşık bir mozaik oluşturmaktır.

Bilgi Platformlarının Yoğunlaşması

İnsanlar düzinelerce yeni bilgi ve veri kanalına eriştiğinden, artık çok fazla bilginin değış tokuş edildiğı temel sosyal medya platformlarının yanı sıra veri yönetimi ve bilgi işleme için ilgili sistemler ve platformlar artık beş büyük şirkette toplanmıştır: Apple, Google (veya ana şirket olarak bilinen Alphabet), Amazon, Facebook ve Microsoft. Bu firmaların her birinin birçok ilgili şirketi vardır: örneğın Google, You-Tube'un, navigasyon uygulaması Waze'in ve akıllı ev ürünleri şirketi Nest'in sahibidir; Facebook, sanal gerçeklik firması Oculus da dahil olmak üzere düzinelerce şirkete sahiptir. O kadar büyük sermaye rezervlerine sahipler ki, tipik olarak yeni başlayan rakipleri satın alabilir ve pazardaki konumlarını koruyabilirler. Kasım 2017 itibariyle, bu beş şirketin piyasa değeri tek başına Nasdaq hisse senedi endeksinin yüzde 40'ından fazlasını oluştuyordu.⁵⁰

The New York Times'tan Farhad Manjoo, bu teknoloji şirketlerini muazzam sosyal güçlerine atıfta bulunarak "korkunç beşli" olarak adlandırdı.⁵¹ Belirli platform hizmetlerine (örneğin çevrimiçi saklama veya sosyal ağ oluşturma) hakim olma biçimleri nedeniyle, temelde kaçınılmaz olan hizmetler sunarlar. Ve bazı durumlarda, iş modelleri ağ etkileri yaratır, bu da platformları ne kadar çok kişi kullanırsa, başkaları için o kadar vazgeçilmez hale geldiklerini ve daha fazla kullanıcıyı kendine çektiğini düşündürür.

Aynı firmalar, giderek yaygınlaşacak olan AI güdümlü, sesle etkinleştirilen kapıcılar (Siri ve Alexa gibi) geliştiriyorlar.

⁵⁰ Conor Sen, "Big Five' Tech Ecosystem'i Yok Edebilir", *Bloomberg*, 15 Kasım 2017.

⁵¹ Farhad Manjoo, "Tech's 'Frightful 5' Öngörülebilir Gelecek için Dijital Yaşama Hakim Olacak," *New York Times*, 20 Ocak 2016.

teknolojiyle etkileşime geçmenin kullanışlı bir yolu. Halihazırda kullanıcılar hakkında önemli veriler topluyorlar - bazen, görünüşe göre, kullanıcıların farkında olmadan. Sorulara verdikleri yanıtların, özellikle tavsiye talebi olarak sorulduğunda objektif olması beklenmemelidir: Bunları geliştiren platformun iş modelinin en iyi avantajını yansıtacaklardır.

Ortaya çıkan bu gerçeklik, son kullanıcıları çeşitli şekillerde etkiliyor. Belki de en önemli etki, bir avuç büyük firmanın Amerikalılar (ve diğerleri) hakkında devasa, birbirine bağlı bilgi veritabanları geliştirmesidir. Bu bilgi birikimi, bu platformların davranış ve tutumları benzeri görülmemiş şekillerde incelemesine ve tahmin etmesine olanak tanır ve reklamcıların tüketicileri kesin bir doğrulukla hedeflemesine yardımcı olur. Bu veritabanları, büyük ölçekli bilgi manipülasyon kampanyalarının bir parçası olarak hırsızlık ve manipülasyona karşı da savunmasızdır.

Bu platformların geniş erişimi, onlara tutumlar üzerinde önemli bir etki de sağlar.⁵² Bu etki derecesi, kısmen, platformların kullanıcı tabanlarını bölümlere ayırma ve sahip oldukları bilgilere dayanarak son derece bireyselleştirilmiş öğelere, hatta bazen belirli bireylere hitap etme yeteneğinin bir ürünüdür. Bu platformlar ve çoklu arayüzleri, kamu algılarının şekillenmesinde baskın bir rol oynadığı ölçüde, benzeri görülmemiş bir etki düzeyine ulaşacaktır.

Yankı Odalarının Rolü

Parçalanmış bir bilgi küresinin eğilimi ile ilgili olarak, yankı odalarının yükselişi vardır: insanların farkındalığını ve bilgi aramasını kısıtlayan, yalnızca mevcut inançlarını destekleyen bilgilerin geçmesine izin veren, kendi kendini tanımlayan bilgi ve inanç siloları. Sosyal medya platformlarındaki veya arama motorlarındaki ayarlar, kullanıcıların gördükleri bilgileri önceki nesillerde olmayan şekillerde uyarlamalarına ve filtrelemelerine olanak tanır ve bu platformlardan bazılarının algoritmaları aynı etkiye sahiptir.

⁵² Ulusal Halk Radyosu, "5 Teknoloji Devi Nasıl Şirketlerden Çok Hükümetlere Benzer Oldu?" *Fresh Air*, 26 Ekim 2017.

"Bunu beğendiyseniz, muhtemelen bundan hoşlanacaksınız" kuralı, yerleşik kalıplara uyan içerik sağlama kuralıdır. Sonuç, bu inançları güçlendirmek ve belki de onları daha yüksek derecelerde aşırılığa teşvik etmek olacaktır.

Bu eğilim üzerine yapılan araştırmalar karışıktır, bu da en azından şu ana kadar yankı odalarının ölçülebilir etkisinin bazı raporların öne sürdüğü kadar büyük olmayabileceğini düşündürmektedir. Bununla birlikte, eğilimin, insanların bilgi araştırmalarını ve ciddiye alınması gereken karşıt görüşlere açıklığını kısıtlama potansiyeline sahip olduğuna dair yeterli kanıt var.

Son zamanlarda yapılan birkaç araştırma, çevrimiçi ortamda kaotik, genellikle ideolojik olarak bölümlere ayrılmış seçenekler menüsüne maruz kalmanın mevcut ideolojik görüşlere yakınlığı artırdığına ve aslında insanların kendilerini karşıt görüşlerden uzak tutmalarına olanak tanıdığına dair kanıtlar bulmuştur.⁵³ Diğer çalışmalar, şaşırtıcı olmayan bir şekilde, siyasi blog yazarlarının ideolojik olarak benzer bloglara bağlanma eğiliminde olduğunu gösteriyor.⁵⁴ Sunstein, yankı odalarının demokrasi için acil bir tehdit oluşturduğunu iddia etmek için kapsamlı araştırmalar yaptı.⁵⁵ Başka bir çalışma, siyasi olarak aktif olan azınlığın karşıt bilgilere dirençli silolarda kilitli kaldığı ve nüfusun çoğunluğunun çok az siyasi haber tükettiği bir duruma "katmanlaşma" riskine işaret ediyor.⁵⁶ Bir çalışma, bir yankı odasının yapacağı gibi, arama sonuçlarında bir siyasi partiyi tercih eden özel olarak çarpık arama motorları yaratma çabalarını inceledi; oylama tercihlerinin yüzde 20'ye varan oranda etkilendiğini buldular.⁵⁷

Pariser, bir yankı odasının nihai biçimi hakkında yazmıştır: Tercihleri hakkında şu anda mevcut olan muazzam verilerden oluşturulmuş, çevrimiçi her kişi için tamamen kişiselleştirilmiş bir bilgi balonu.

53 Çevrimiçi ideolojik yaklaşmayı gösteren bir çalışma, Diana C. Mutz ve Paul S. Martin, "Facilitating Communication Across Lines of Political Difference: The Role of Mass Media," *American Political Science Review*, Cilt. 95, No. 1, 2001.

54 Lada Adamic ve Natalie Glance, "The Political Blogosphere and the 2004 US Election: Divided They Blog", Weblog-ging Ecosystem üzerine İkinci Yıllık Çalıştayda sunulan bildiri, Chiba, Japonya: Association for Computing Machinery, 2005.

55 Sunstein, 2017.

56 W. Lance Bennett ve Shanto Iyengar, "A New Era of Minimal Effects? Siyasal İletişimin Değişen Temelleri," *Journal of Communication*, Cilt. 58, No. 4, 2008.

57 O'Neil, 2016, s. 184.

Böyle bir durumda “kimliğiniz medyanızı şekillendirir” ve “medyanız o zaman neye inandığınızı ve neye önem verdiğinizi şekillendirir” diyor. Tıklama, arama ve alışveriş, bilginin uyarlanmasını keskinleştirmek için kullanılabilecek daha fazla veri üretir, aslında bilgi balonunun duvarlarını sertleştirir. "Bir sen döngüsüne hapsolursun ve kimliğiniz yanlış temsil edilirse, bir amplifikatörden gelen yankı gibi garip kalıplar ortaya çıkmaya başlar." Ve açıkladığı gibi, büyük veri ve yapay zekanın birleşimi, yıldırım hızında böyle tekil baloncuklar oluşturma potansiyeli yaratıyor: "Sistem sizden ne kadar hızlı öğrenirse, bir tür kimlik çağlayanına hapsolme olasılığınız o kadar artar. . . . küçük bir ilk eylemin” sizi belirli bir insan türü olarak damgaladığı ve ortaya çıkan yankı odasını yoğunlaştırdığı. ⁵⁸

İnternet bu etkilere sahip olma konusunda yalnız değildir ve hatta bunların en önemli nedeni bile olmayabilir. Partizan televizyon ağları şu etkiyi yaptı: Fox News ve MSNBC izleyicileri zaman içinde ideolojik olarak daha kutuplaştı. Bir grup araştırmacı, sosyal kimlik teorisini kullanarak, kısmen oldukça olumsuz reklamlar nedeniyle Amerika Birleşik Devletleri'nde siyasi kutuplar arasındaki hoşnutsuzluğun önemli ölçüde arttığını gösterdi. ⁵⁹ Başka bir araştırma, insanların ideolojik olarak uyumlu bir ağıla ilişkiliyse bir başlıkla daha fazla ilgilendiğini buldu. Araştırmalar, Twitter kullanıcılarının benzer görüşlere sahip kişilerle daha sık etkileşime girdiğini, insanların görüşlerini destekleyen hikayelerle manşetlere çekildiğini ve Facebook kullanıcılarının görüşlerini doğrulayan bilgilere tıklama veya “beğenme” olasılığının çok daha yüksek olduğunu gösteriyor. ⁶⁰

Sunstein ayrıca, yankı odalarının olası sonucunu gösteren endişe verici bir sosyal bilim araştırması çizgisine işaret ediyor: *grup kutuplaşması olarak bilinen bir fenomen üzerinde çalışın* . Uzun zamandır insanları sorunları tartışmak için gruplara ayırmanın fikirleri yumuşatacağına inanılıyordu. Bununla birlikte, çok sayıda çalışma, grupların , bireylerin grup toplantısından önce ifade ettikleri tutumlarla karşılaştırıldığında, önceden sahip olduklarından *daha fazla aşırı tutum üretme eğiliminde olduğunu bulmuştur*.

⁵⁸ Pariser, 2011, s. 125–127.

⁵⁹ Shanto Iyengar, Guarav Sood ve Yphtach Lelkes, “Affect, Not Ideology: A Social Identity Perspective on Polarization,” *Public Opinion Quarterly* , Cilt. 76, No. 3, 2012.

⁶⁰ Sunstein, 2017, s. 61, 64–65, 81, 114–115, 119–126.

günlükler. ⁶¹ Bu bulgu, ideolojik olarak tutarlı olmayan gruplar için bile doğrudur, ancak bu tür insanların yankı odalarının bu konuda daha da büyük bir etkiye sahip olması beklenebilir. Gerçekten de Sunstein, grup kutuplaşması etkilerinin çevrimiçi olarak gerçekleştiğini gösteren araştırmalardan alıntı yapıyor.

Önemli bir çalışma bu etkileri doğrulamaktadır. Araştırmacılar, aşırı ve kutuplaşmış görüşlerin olasılığını sunan parçalanmış bir bilgi bağlamının varlığının bilgi arama nasıl etkileyeceğini ve bunun sonucunda “duygusal kutuplaşma”yı nasıl etkileyeceğini incelemeye çalıştılar: karşıt siyasi grupların üyelerinin ne dereceye kadar sert bir şekilde olumsuz bir ışık altında görüldüğü. Gerçekten de, “isteğe bağlı bilgi arama”nın - son derece parçalanmış bir bilgi ortamında kutuplaşmış, doğrulayıcı kanıt arama yeteneğinin - bu tür duygusal kutuplaşmayı yüzde 15'e kadar artırma etkisine sahip olduğunu buldular. ⁶² İlgili bir araştırma, geniş bant internete erişimin ve dolayısıyla daha geniş bir dizi potansiyel bilgi kaynağının (yüksek düzeyde kutuplaşmış olanlar dahil) duygusal kutuplaşmayı artırdığını bulmuştur. ⁶³ Başka bir araştırma, Facebook arkadaşlarının, kendi seçtikleri grupların mevcut inançlarını güçlendiren haber hikayelerini ve diğer bilgileri vurgulama eğiliminde olduğunu buldu. ⁶⁴

Yine de, bu tür kanıtlarla bile, yankı odaları üzerine yapılan araştırmaların bulguları oldukça çelişkili olmaya devam ediyor. Sunstein'ın belirttiği gibi birçok araştırma, birçok insanın “yankı odalarından hoşlanmadığını” öne sürüyor. . . . [M]halkın herhangi bir üyesi, kendilerinden farklı olan bakış açılarını görmekle yakından ilgileniyor.” ⁶⁵ Ekonomistler tarafından yapılan kapsamlı bir çalışma Gentz-

⁶¹ Sunstein, 2017, s. 68–69, 77–78. Literatürün gözden geçirilmesi için bkz. Daniel J. Isenberg, “Group Polarization: A Critical Review and Meta-Analysis,” *Journal of Personality and Social Psikoloji*, Cilt. 50, No. 6, 1986.

⁶² Richard R. Lau, David J. Andersen, Tessa M. Ditonto, Mona S. Kleinberg ve David P. Redlawsk, “Effect of Media Environment Diversity and Advertising Tone on Information Search, Selective Exposure, and Affective Polarization,” *Politik Davranış*, Cilt 39, Sayı 1, 2017.

⁶³ Yphtach Lelkes, Guarav Sood ve Shanto Iyengar, “The Hostile Audience: The Effect of Access of Broadband Internet on Partizan Effect,” *American Journal of Political Science*, Cilt. 61, Sayı 1, 2017.

⁶⁴ Eytan Bakshy, Solomon Messing ve Lada Adamic, “Possure to Ideologically Diverse News and Opinion on Facebook,” *Science*, Cilt. 348, No. 6329, 2015.

⁶⁵ Sunstein, 2017, s. 5.

kow ve Shapiro, insanların yalnızca hemfikir oldukları web sitelerini ziyaret etme derecesini veya “izolasyon indekslerini” ölçmeyi amaçladı. (Tüm zamanlarını Fox News'de geçiren muhafazakarların izolasyon endeksi 100'dü.) Araştırmaları, kendini muhafazakar olarak tanımlayanların çevrimiçi ortalama izolasyon endeksinin yüzde 60,6 ve kendini liberal olarak tanımlayanların yüzde 53,1 olduğunu buldu. ⁶⁶ Başka bir araştırma, insanların çevrimiçi haber tüketiminin “olağanüstü derecede bir denge” gösterdiğini buldu. ⁶⁷ 50.000 kişinin göz atma alışkanlıkları üzerine yapılan büyük bir araştırma, kalıpların ideolojik boşlukları yansıttığını, ancak bu boşlukların çoğunlukla yerleşik ana akım medya sitelerine yapılan alışılmış ziyaretlerin bir ürünü olduğunu buldu. Aslında, genel tarama, onları çevrimdışı haber tüketiminden daha az farklı görüşten ziyade daha fazlasıyla temasa geçirdi. ⁶⁸

Pew Araştırma Merkezi tarafından yapılan son anket, yankı odaları konusunda birkaç bakış açısı sunuyor. Bir anket, insanların haberleri için birden fazla sosyal medya sitesi kullandığını gösteriyor ve bu da onların silolarda sıkışıp kalmayabileceklerini gösteriyor. ⁶⁹ Başka bir anket, sosyal medya kullanıcılarının yalnızca yüzde 9'unun “hükümet politikası hakkında sık sık tartıştığını, yorum yaptığını veya paylaşımında bulunduğunu” söylediğini, çevrimiçi ortamların çoğunlukla siyasi olmadığını ve bu nedenle siyasi görüşler üzerinde hafif etkileri olabileceğini belirtti. Aynı anket, çoğu insanın sosyal medyadaki arkadaş gruplarının farklı bakış açılarından insanlar içerdiğini bildirdiğini buldu.

⁷⁰

2013'te yapılan önemli bir araştırma, çevrimiçi ortamda "savunma amaçlı kaçınma" konusunda çok az kanıt buldu; yani, kişinin siyasi inançlarıyla uyuşmayan içeriğe sahip sitelerden kaçınma modeli. İdeolojik olarak tanımlanmış siteleri ziyaret eden kişilerin ana akım siteleri ziyaret etme olasılığı daha yüksekti.

⁶⁶ Matthew Gentzkow ve Jesse M. Shapiro, “İdeolojik Ayrım Çevrimiçi ve Çevrimdışı,” *Quarterly Journal of Economics*, Cilt. 126, Sayı 4, 2011.

⁶⁷ Andrew M. Guess, *Medya Seçimi ve Denetleme: Çevrimiçi İzleme Verilerinden Kanıtlar*, iş piyasası raporu, New York: New York Üniversitesi, 6 Eylül 2016.

⁶⁸ Seth Flaxman, Sharad Goel ve Justin M. Rao, “Filter Bubbles, Echo Chambers ve Online News Consumption,” *Public Opinion Quarterly*, Cilt 80, Sayı S1, 2016.

⁶⁹ Elizabeth Grieco, “Daha Fazla Amerikalı Haber İçin Birden Fazla Sosyal Medya Sitesine Dönüyor,” *Pew Araştırma Merkezi*, 2 Kasım 2017.

⁷⁰ Maeve Duggan ve Aaron Smith, “Sosyal Medyadaki Politik Ortam,” *Pew Araştırma Merkezi*, 25 Ekim 2016, s. 7.

ve hatta “ideolojik olarak tutarsız” olanlar.⁷¹ Bazı araştırmalar, insanların inançlarıyla uyumlu bilgiler arama eğilimindeyken, kendi görüşlerine aykırı bilgilerden aktif olarak kaçındıklarına dair çok az kanıt olduğunu öne sürüyor.⁷² Diğer araştırmalar, çevrimiçi siyasi bilgi arayan kişilerin, çoğunlukla yayın ve ana akım medyaya güvenenlere göre ideolojik olarak daha aşırı olma eğiliminde olduğunu ortaya koyuyor.⁷³ Bu mantıklıdır—politik olarak aktif insanlar bilgi için piyasada olacak ve onu toplamak için daha fazla adım atacaktır—ancak bu aynı zamanda çevrimiçi kullanıcıların daha fazla kutuplaştığını gösteren bulguların neden değil, bir semptom gösterebileceği anlamına gelir. Konuyla ilgili kapsamlı çalışmalar yapan iki bilim adamı, “gerçek okuyucu davranışına dayanan şu ana kadarki en iyi kanıt, İnternet'teki ideolojik ayrımcılığın sınırlı olduğunu öne sürüyor” sonucuna varıyor. Ayrıca, internette ayrışma riskinin nispeten yeni bir tehdit olduğunu ve bunu zaman içinde azaltacak birçok politika tepkisi olabileceğini vurguluyorlar.⁷⁴

Yine de bu kanıtların toplamı, parçalanmış bir bilgi ortamından kendi kendini doğrulayan kanıtlar toplayan, giderek izole edilmiş kutuplaşmış grupların gerçek tehlikesine işaret ediyor. Üç bilim insanının yükselen bilgi dünyasını özetlediği gibi: “Şu anda nüfusun büyük bir bölümünün geleneksel kanıt, iç tutarlılık ve gerçek arayışı kriterlerini terk eden epistemik bir alanda yaşadığı bir durumla karşı karşıyayız.” Devam ediyorlar:

71 R. Kelly Garrett, Dustin Carnahan ve Emily K. Lynch, “Kaçınmaya Doğru Bir Dönüş mü? Selective Exposure to Online Political Information, 2004–2008,” *Politik Davranış*, Cilt. 35, No. 1, 2013, s. 113–134.

72 R. Kelly Garrett, “Echo Chambers Online?: İnternet Haber Kullanıcıları Arasında Politik Motivasyonlu Seçici Maruz Kalma”, *Journal of Computer-Mediated Communication*, Cilt. 14, No. 2, 2009a. Ayrıca bkz. R. Kelly Garrett, “Politik Motivasyonlu Güçlendirme Aramak: Seçici Maruz Kalma Tartışmasını Yeniden Çerçevelemek,” *Journal of Communication*, Cilt. 59, No. 4, 2009b.

73 Norman H. Nie, Darwin W. Miller III, Saar Golde, Daniel M. Butler ve Kenneth Winneg, “The World Wide Web and the US Political News Market,” *American Journal of Siyaset Bilimi*, Cilt. 54, Sayı 2, 2010.

74 R. Kelly Garrett ve Paul Resnick, “İnternetteki Politik Parçalanmaya Karşı Direnmek,” *Daedalus*, Cilt. 140, No. 4, Güz 2011.

Post-truth dünyasının bariz bir özelliği, gerçeklerin ve nesnel kanıtların mevcut inançlar ve önyargılar tarafından gölgede bırakıldığı, insanlara kendi gerçekliklerini seçme yetkisi vermesidir. Bu, aldatma ve aldanmayı destek toplamak için yeterli araç olarak modelleyen liderler tarafından güçlendirilebilir. Bu dünyada yalan sadece kabul edilmez, ödüllendirilir de. Gerçeği tahrif etmek artık insanların inançlarını değiştirmekle ilgili değil, gücü öne sürmekle ilgili.⁷⁵

Sonuçta ortaya çıkan, kendi görüşlerini destekleyen bilgilerle silahlanabilen kendi kendine ayrılmış gruplar ve bu grupların görüşlerinde giderek aşırı ve kutuplaşmış hale gelmesi, ortaya çıkan bilgi bağlamının önde gelen tehlikelerinden biridir. Göreceğimiz gibi, aynı zamanda düşmanca sosyal manipülasyon çabalarının bugüne kadar güçlü bir şekilde dayandığı temeldir.

Etkileyenlerin Rolü

Silolar fikriyle ilgili olarak, daha geniş bir *etkileyici kavramı vardır* : bilgi ağlarında kilit düğümler olarak işlev gören ve bilgi akışları ve inanılan ve dolaşımda olan şeyler üzerinde orantısız etki uygulayan insanlar veya küçük gruplar. Araştırmalar, herhangi bir sosyal medyadaki veya diğer bilgi ağındaki insanların küçük bir bölümünün bilgi paylaşımının önemli bir bileşenini oluşturacağını gösteriyor.

Kritik soru, etkileşim kalıplarının nasıl ortaya çıktığıdır - büyük ağ bağlantılı kalıplarda meydana gelen kümelenmeyi veya gruplamayı ne etkiler. Sosyal ağlardaki bu kümeler genellikle etkili bireyler veya gruplar veya genellikle etkileyici olarak adlandırılan bilgi kaynakları etrafında gerçekleşir. Albert-László Barabási, ortaya çıkan aktörleri *bağlayıcılar* ve *merkezler* olarak adlandırdı . Ağlardaki “anormal derecede fazla sayıda bağlantıya sahip düğümler” olarak tanımladığı bağlayıcılar, “trendler ve modalar yaratmaya, önemli anlaşmalar yapmaya, modaları yaymaya veya bir restoran başlatmaya yardımcı olmaya” hizmet ediyor. Örneğin, özellikle etkili doktorlar, kendi alanlarında orantısız bir düşünce düzeyinden sorumludur. Çevrimiçi dünyada, araştırmalar nispeten küçük bir

⁷⁵ Lewandowsky, Ecker ve Cook, 2017, s. 360–361.

Amazon ve Yahoo gibi çok sayıda hub aynı işlevi görür. Tüm amaçlarla yalnızca birkaç başka yere bağlanan sayfalar “yoktur”; sadece hub'lar üzerinden büyük paylaşımlar yoluyla haberler viral olarak yayılır. ⁷⁶

Bu kesişen eğilimlerin olası bir sonucu, bilgi akışlarının daha çok kendi seçtikleri yankı odalarına bağlı olduğu ve etkileyiciler tarafından şekillendirildiği sosyal medyanın, genel haber tüketiminden çok daha yüksek dozda dezenformasyon yansıtmasıdır. Örneğin, 2018'de Avrupa'da haber tüketimi üzerine yapılan bir araştırma, uydurma veya abartılı iddialar üzerine kurulmuş haber sitelerinin “gerçek” haber sitelerinin ilgisinin yalnızca çok küçük bir bölümünü çektiğini buldu. Hiçbir yanlış haber sitesi, nüfusun yüzde 3,5'inden fazla bir aylık erişime sahip değildi ve çoğu, büyük gazete sitelerinin yüzde 22 ile yüzde 51'i arasındaki erişime kıyasla çok daha düşüktü. Yine de Facebook'ta, "en popüler haber markalarının ürettiğiyle eşleşen veya aşan az sayıda yanlış haber kaynağı tarafından oluşturulan" toplam etkileşim ölçümleri. ⁷⁷

Trol Etiği

de yüzbinlerce hatta milyonlarca internet kullanıcısı tarafından *trolling etigi* olarak adlandırılabilir şeyin yaygınlığıdır . Bu terim, geleneksel çevrimiçi diyalogu bozmak, yaramazlık yaratmak ve tartışmayı yoğunlaştırmak için abartılı veya icat edilmiş hikayeler, hicivli memler ve bazen kısır saldırılar kullanma çabasını tanımlar. Medya ortamının sansasyonelliğini mizahi, yıkıcı ve saldırgan amaçlarla kullanmaya kararlı ironik ve küstah bir zihniyettir. Bazı yönlerden troller, modern internetteki sansasyonelizm ve

⁷⁶ Barabasi, 2014, s. 56–58; doktor etki merkezlerine yapılan atıf s. 129.

⁷⁷ Richard Fletcher, Alessio Cornia, Lucas Graves ve Rasmus Kleis Nielsen, *Measuring Avrupa* , Oxford, Birleşik Krallık'ta “*Sahte Haber*” ve *Çevrimiçi Dezenformasyonun Erişimi* : Reuters Gazetecilik Araştırmaları Enstitüsü, Oxford Üniversitesi, Şubat 2018.

yankı odaları. Bilgin Whitney Phillips'in belirttiği gibi onlar, “sosyal ağlar dünyasının yüzünü buruşturan poster çocukları”.⁷⁸

Trolleme etiği için tanımlayıcı web kolektifi, 4chan sitesidir ve özellikle onun kötü şöhretli “/b/” panosu, sorunlar, web siteleri ve bireyler hakkında bir dizi ironik, düşmanca ve parodik yorum için sıfır noktasıdır. 2008 ve 2010 yılları arasında 4chan, günde 8 milyondan fazla sayfa görüntüleme, ayda 200 milyon ziyaretçi ve 400.000 günlük gönderi olarak büyük bir web varlığı haline geldi.

⁷⁹

Troller artık bir dizi ünlü kampanya ve saldırıya giriştiler. Daha saf ironik ve mizahi yollarla, aptal ve anlamsız web mizah sitelerine karşı devam eden taciz kampanyaları düzenlediler. Hacker kolektifi “Anonim”, özellikle 4chan topluluğundaki trol hareketinde köklere sahiptir, ancak sonunda “gerçek dünyada” daha aktif bir varlık haline gelmek için resmi protestolar düzenleyerek ve bir dizi yıkıcı saldırıyı sürdürerek ayrıldı. ve trolleme kampanyaları. Rastgele çevrimiçi forumlar ve şirketler gibi hedeflere saldırdılar.

Daha kötü bir ifadeyle, troller, “anlamadıklarını” düşündükleri bireylere karşı en iğrenç siber zorbalık biçimlerini başlatmak ve trollük etiğine karşı çıkmak için bir araya geldiler. Sürecin en uğursuz örneklerinden birinde, internet trolleri, Facebook'ta veya başka yerlerdeki anıt sitelere acımasız ve genellikle müstehcen yorumlar gönderdikleri bir "RIP trolling" pratiği başlattılar, hatta bunu yapan çocukların ailelerine saldırdılar. trajik bir şekilde ölmüştü.

Bu tür saldırılar anlaşılabilir görünebilir, ancak Whitney Phillips'in işaret ettiği gibi, trol hareketinin en önemli yönlerinden biri “duygusal ayrışma”dır. Pek çok trol, sanal ve gerçek benlik arasında keskin bir ayrım yaptıkları için çevrimiçi olarak düşmanca saldırılar gerçekleştirir. Phillips'in araştırmasından elde ettiği bilgilere göre, çoğu gerçek hayatta sessiz, düşünceli ve saygılı, çevrimiçi oldukları şekilde asla yüz yüze saldırılara girişmeyeceklerinde ısrar eden kişilerdir.

⁷⁸ Whitney Phillips, *Bu Neden Güzel Şeylere Sahip Olamadığımız: İlişkinin Haritasını Çıkarmak Online Trolling ve Mainstream Culture Arasında*, Cambridge, Mass.: MIT Press, 2015, s. 8; bkz. ayrıca s. 5-6.

⁷⁹ Phillips, 2015, s. 55-56.

“Trol benliklerinin ve çevrimdışı ('gerçek') benliklerinin tamamen farklı kurallar dizisine tabi olduğu konusunda ısrar ediyorlar.”⁸⁰

Bu ayrım ahlaki açıdan sakıncalı olabilir, ancak trollerin çevrimiçi ortamda çarpıcı biçimde farklı davranışları haklı çıkarmasına olanak tanır. Ve bu tür uygulamalar aslında daha geniş bir çevrimiçi ayrışma pratiğiyle ve dikkat çekmek için sansasyonel içerikle oynamayla yakından ilişkilidir. "Tıklama tuzağı" fikri, "trol tuzağı"ndan sadece bir adım ötededir; her iki durumda da fikir, anlamlı bir içerik sunmaktan ziyade dikkat çeken içerik üretmektir. Her iki durumda da örüntü, kısmen yabancılaşmış bireyler ya da grupların sistemin “geleneksel” etiği ve kurumları olarak algıladıklarına saldırmasıdır.

Bu tür trolleme ve taciz küresel hale geldi ve hem devlet hem de devlet dışı birçok uluslararası aktör tarafından zorlayıcı amaçlarla kullanıldı. Haroon Ullah, aşırılık yanlılarının siyasi liderlerin güvenilirliğini sarsmak için sahte videolar oluşturma yöntemlerinin yanı sıra radikal yaşam tarzına yönelik tanıtım videolarını da listeliyor. Aşırılıkçılıkla modern savaş, çoğu aşırılıkçı mesaja karşı çıkanları taciz etmek ve itibarsızlaştırmak için trolleme taktikleri kullanan bilgi kanallarının hakim olduğu bir şekilde tasvir ediyor.⁸¹

Veri Kuralı

Son olarak, bilgi dünyası, pazarlama algoritmalarından sağlık hizmetleri kararlarına ve eğitim seçimlerine kadar her şeyi yönlendirmek için kullanılan devasa veritabanlarının birikmesi ve manipülasyonu ile giderek daha fazla karakterize ediliyor. Bu veritabanları, yapay zekanın ve birçok alanda giderek artan algoritmik karar vermenin temeli haline geliyor.

Pek çok şirket, bireysel Amerikalılar hakkında çok büyük veri hazinelerini bir araya getiriyor. Facebook, 1.300'den fazla benzersiz kategoriye hedefleyebilmesiyle övünür. Amazon'un Alexa'sı satın almalar hakkında bilgi toplar, aynı zamanda insanların evlerinde aktif olduğu için “uyandığınızda,

⁸⁰ Phillips, 2015, s. 33–35.

⁸¹ Haroon K. Ullah, *Dijital Dünya Savaşı: İslamcılar, Aşırılıkçılar ve Siber Mücadele Supremacy*, New Haven, Conn.: Yale University Press, 2017, s. ix–xv.

ne izlediğini, okuduğunu, dinlediğini, istediğini ve yediğini.” Kişisel telefonlardan toplanan verilere dayanarak, reklamcılar "genellikle günün hangi saatlerinde gezindiğinizi, video izlediğinizi, e-postaları yanıtladığınızı, ofise seyahat ettiğinizi ve hangi seyahat rotalarını kullandığınızı" bilirler. İnsanların seyahatlerinde ne tür otellerde kaldıklarını ve dünyanın hangi bölgelerini ziyaret etmekle ilgilendiklerini biliyorlar. Bu tür veriler, AI güdümlü pazarlamayı besleyebilir: Bu tür kesin tercih bilgileriyle donanmış olarak, "[m]akineler, tıpkı makinelerin arabaları sürmesi gibi reklamlar yapacaktır." ⁸²

Pariser, "Çok az bir uyarı veya tantanayla," diye savundu, "dijital dünya temelden değişiyor. Bir zamanlar herkesin herhangi biri olabileceği anonim bir ortamdı. . . artık kişisel verilerimizi talep etmek ve analiz etmek için bir araçtır." ⁸³ Ne zaman biri seyahat rezervasyonu yapsa, çevrim içi sözlükte bir kelime aratsa, herhangi bir şey aratsa, sosyal medya gönderisi yapsa, çevrim içi bir şey satın alsa ya da herhangi bir faaliyette bulunsa, şirketler binlerce bilgiyi çöpe atıyor ve bireylerin portrelerini bir araya getirmek. Bu bilgi toplama, önde gelen internet şirketlerinin çoğunun tanımlayıcı iş modelidir ve Acxiom ve Cam-bridge Analytica gibi uzman firmalar, her Amerikalı hakkında binlerce ayrık bilgi derler. Bu bilgi, aile ve arkadaşların adlarını, kredi geçmişini ve satın alma geçmişini, kredi kartı bakiyelerini, evcil hayvan sahipliğini ve bireylerin hemen hemen tüm diğer ölçülebilir özelliklerini içerebilir. Bu tür veri tabanlarını kullanarak özel şirketler, günlük rutinimizden satın alma tercihlerimize kadar yaşam modellerini izleyebilecek ve tahmin edebilecek. ⁸⁴

Çalınan veriler, sosyal manipülatörlerin araç setinin önemli bir unsuru olabilir. Önde gelen bir örnek, Amerikalılara şantaj yapmak için kullanılabilecek, Personel Yönetimi Ofisinden bilgi hırsızlığıdır. İddia edilen Çinli izinsiz giriş, personel dosyalarını, dijital parmak izlerini, Sosyal Güvenlik numaralarını ve daha fazlasını açladı. Geleneksel bir siber saldırıda, bir saldırgan bilgiyi "kilitlemek" için kullanabilir.

⁸² Ken Auletta, "Matematik Adamları Deli Adamları Nasıl Devirdi?" *New Yorker* , 21 Mayıs 2018.

⁸³ Pariser, 2011, s. 6.

⁸⁴ Stacey Higginbotham, "IBM, Nesnelerin İnternetini Fethetmek için Watson'ı Getiriyor," *Fortune* , 15 Aralık 2015.

tıbbi kayıtlar, finansal bilgileri silip süpürür, sosyal medyayı manipüle eder ve kişisel suistimaller hakkında yalanlar ve yarı gerçekler yayar.” Saldırgan, arkadaşlarını ve akrabalarını taciz edebilir ve hatta Twitter üzerinden ölüm tehditleri gönderebilir.⁸⁵ Ancak daha aşamalı bir sosyal manipülasyon biçiminde, bir saldırgan, rakip bir toplumun dışlılarına daha fazla kum katmaya yetecek kadar kafa karışıklığı, hayal kırıklığı ve endişe yaratmak için ayda yüzlerce şey yapabilir, ancak hiçbir zaman o dereceye ulaşmadan. büyük ölçekli bir siber saldırı olarak sayılabilecek bir manipülasyon.

Özet: Gelişmiş Demokrasiler İçin Değişen Bir Bilgi Ortamı

Bu eğilimler, ortaya çıkan bilgi dünyasının gelişmiş sosyal manipülasyon kampanyalarına karşı savunmasız olabileceği çeşitli yollara işaret ediyor. Eğilimler, ortaya çıkan bir bilgi ortamını tasvir ediyor.

- parçalanmış ve merkezi olmayan, önemli ölçüde yankı odası etkisine tabi olan ve sosyal algıları birleştiren ve insanlara siyasi bir topluluğa temel ve aidiyet duygusu veren büyük anlatılardan yoksun
- giderek daha fazla ağ bağlantılı ve birbirine bağlı ve bireysel Amerikalılar hakkında geniş bir veri hazinesi üzerinde oturan bir avuç büyük teknoloji firması tarafından sağlanan platformlara bağımlı ve bu da birlikte artan derecede sistemik risk yaratıyor
- önemli derecelerde sansasyonel haberler ve sosyal medyada katılımcıların düşmanca trollenmesi ve taciz edilmesi ile karakterize edilir.

Sonuç, sosyal tutarlılığı baltalayan şekillerde giderek daha fazla parçalanmış, ağlara bağlı zayıflıklar yaratacak şekillerde birbirine bağlanan ve halkın algılarını sürekli olarak çarpıtan ve ontolojik güvenliği, geleceğe olan güveni, güveni, ve sosyal kurumlar. Hatta önce

⁸⁵ Ian Brown, "Bir Siber Sürpriz Hayal Etmek: Çin Güveni Hedeflemek için Çalınan OPM Kayıtlarını Nasıl Kullanabilir?" *Kayalarda Savaş*, 22 Mayıs 2018.

Bir ülkenin bilgi dünyasını manipüle etmek için dışarıdan alınan aktif, düşmanca önlemleri düşünüyoruz, kanıtlar temel eğilimlerin zaten demokratik kurumlar ve sosyal istikrar üzerinde yıpratıcı etkileri olabilecek bir bilgi ortamı oluşturduğunu gösteriyor. Başka bir deyişle sorun, her şeyden önce değişen bilgi küresinden biridir ve yalnızca ikincil olarak sosyal manipülasyon ölçütleridir.

Sosyal Bilimlerden Görüşler

Bu noktaya kadar, ortaya çıkan bilgi ortamının karakterini ve bu gelişen bilgi küresinin silahlandırılması için olası sonuçları gözden geçirdik. Sosyal manipülasyonun temelini ve etkilerini daha iyi anlamak için, konuyla ilgili çeşitli araştırma alanlarını da inceledik. Bu noktada bariz bir örnek bilişsel ve sosyal psikolojidir. Sosyal manipülasyonun etkililiği hakkında ne söylemek zorunda ve sosyal manipülasyonun etkililiğine karşı koymak için ne yapılabilir?

Bu bölümdeki analiz, Christopher Paul ve Miriam Matthews tarafından Rus dezenformasyon teknikleri üzerine önceden yapılmış bir RAND çalışmasına dayanmaktadır. Bu çalışma, Rus propagandacıları tarafından kullanılan yaklaşımları değerlendirmek için zemin hazırlamak için sosyal bilimler literatürünün tutumlar, iknalar ve inanç sistemleri hakkındaki önemli bulgularını gözden geçirdi. ¹ Bu bölümün amacı biraz daha geniş bir odakla aynıdır: sosyal bilimlerde yerleşik bulguların sosyal manipülasyonun geleceği hakkında ne anlama gelebileceğini anlamak.

Bu alanın temel dersi, epistemolojinin temel bir yönüdür: Bilgi ve anlama, *yorumlayıcı* eylemlerdir. İnsanoğlu sürekli olarak karşılaştığı gerçekleri anlamlandırmaktadır. Bu gerçeklerin en önemli yönü, onların “nesnel” geçerliliği değil, insanların onlardan ne anladığıdır. Bu sürekli süreç, daha büyük *bilişsel cimrilik* olgusunun bir ürünüdür. İnsanlar bombalanıyor

1 Christopher Paul ve Miriam Matthews, “Rus 'Yanlışlığın Yangın Hortumu' Paganda Yanlısı Model: Neden Çalışabilir ve Karşı Çıkmak İçin Seçenekler,” Santa Monica, Kaliforniya.: RAND Corporation, PE-198-OSD, 2016.

işleyebileceklerinden çok daha fazla bilgi. Sürekli olarak kısayollar için pazardalar: özellikle belirli gerçeklerin geçerliliğini yargılayarak, gelen selden anlam çıkarmanın yolları. İnsanlar, gelen bilgileri yerleşik dünya görüşlerine uydurmak, güvenilir olduğuna inandıkları kaynaklardan gelen bilgileri kabul etmek ve "kalabalığa katılmak" gibi çeşitli teknikleri kullanırlar. Bu kısayollar, sosyal manipülasyon kampanyalarının potansiyel etkinliğini sınırlar: İnsanları desteklemek istedikleri önceden belirlenmiş inançlardan uzaklaştırma çabaları çok zor olabilir.

Gerçekten de, *motive edilmiş akıl yürütme* —bilgiyi nesnel olarak değerlendirmek yerine halihazırda ulaştığımız sonuçları desteklemek için kullanmak— insan düşünme biçimlerinin temelidir. 2 Araştırmalar, bir doğruluk motivasyonu olduğunu öne sürüyor - insanlar “doğru” bilgiye sahip olmak istiyorlar - ancak bu motivasyon, birçok durumda daha güçlü olan motivasyon olan mevcut bakış açılarını sürdürmek ve güçlendirmek için dengeleyici bir dürtü ile sürekli savaş halindedir. 3 Sonuç, süregelen bir “sınırlı rasyonellik” alışkanlığı ve bazen kasıtlı olarak manipüle edilebilecek yanlış algılamadır.

İnsan bilişinin bu temel doğası, sosyal manipülasyon için tartışmasız en önemli giriş noktasını üretir: İnanç ve beklenti, insanların olayları ve gerçekleri algıladıkları merceği yaratır. İnanç, birçok yönden ve çoğu durumda gerçeklerden daha güçlüdür. 4 Bu, bir popülasyon içindeki alt grupların inanç sistemleri şeklinde, yukarıda açıklanan tüm araç ve tekniklerle şekillendirmek için hammadde ile potansiyel bir sosyal manipülatör sağlar. Göreceğimiz gibi, çoğu zaman birçok insanda belirli bir doğruluk motivasyonu vardır. Ancak bu son derece olumsuzdur ve bazı gruplarda bazen tamamen önyargılara yol açabilir.

2 Güdülenmiş akıl yürütme üzerine temel bir kaynak Kunda, 1990'dır. Yanlış bilgiyle bağlantı için, bkz. John Cook, Ulrich KH Ecker ve Stephan Lewandowsky, “Neutralizing Misinformation Through Inoculation: Expositioning Misleading Argumentation Techniques Its Influence”, *PLOS One*, Cilt. 12, Sayı 5, 2017, s. 2.

3 Flynn, Nyhan ve Reifler, 2017, s. 131–135.

4 Elizabeth Kolbert, “Neden Gerçekler Fikrimizi Değiştirmiyor,” *New Yorker*, 27 Şubat 2017; Troy Campbell ve Justin Friesen, “Neden İnsanlar 'Gerçeklerden Uçuyor’” *Scientific American*, 3 Mart 2015.

ve önyargılar, yetenekli sosyal manipülatörlerin hedeflerine ulaşmak için kullanabilecekleri bilişsel hatalar.

Tutumlar ve Tutum Değişikliği

Tutum, bireyin belirli bir nesne, konu veya kişi ile o şeye ilişkin “özet değerlendirmesi” arasındaki ilişkidir. ⁵ Bir tutumun en önemli yönü, bir kişinin genel olarak konuya karşı olumlu mu yoksa olumsuz mu hissettiğini değerlendiren yargıdır. Sosyal psikoloji, siyaset bilimi ve reklamcılıkta tutum değişikliği üzerine, tümü büyük ölçüde bilişsel psikolojiden yararlanan ilgili literatürler vardır. ⁶

Özellikle siyasi ideoloji ve benzeri konularda derinden tutulan kişisel tutumlar, değişime “dikkate değer ölçüde” dirençlidir. ⁷ Kişi bir kez bilgiyi içselleştirip bir inanç oluşturduktan sonra, düşüncesini değiştirmek zordur.

5 Gregory R. Maio ve Geoffrey Haddock, *The Psychology of Attitudes and Attitude Change*, Thousand Oaks, California: SAGE Publications, 2009, s. 4. Sosyal psikolojideki “tutum” kavramı hakkında daha fazla bilgi için bkz. Richard E. Petty, Russell H. Fazio ve Pablo Briñol, eds., *Attitudes: New Implicit Measures from Insights from the New Implicit Measures*, New York: Psychology Press, 2008.

6 20. yüzyılın başlarından ortalarına kadar olan sosyal psikolojinin çoğu, tutumların incelenmesine ve daha spesifik olarak onları tanımlamaya ve ölçmeye odaklanmıştır; Herbert C. Kelman, “Tutumlar Canlı ve İyidir ve Eylem Alanında Kazançla İstihdam Edilir,” *Amerikan Psikolog*, Cilt. 29, No. 5, 1974. Tutumlarla ilgili ilk çalışmalardan biri Gordon Allport'un *Tutumu*, “deneyim yoluyla düzenlenen ve bireyin ilişkili olduğu tüm nesne ve durumlara tepkisi üzerinde yönlendirici bir etki uygulayan zihinsel ve sinirsel bir hazır olma durumu” olarak tanımladığı 1935 tarihli çalışmasında; Gordon Allport, “Attitudes”, Carl Murchison, ed., *A Handbook of Social Psychology*, Worcester, Mass.: Clark University Press, 1935, s. 798; Garth S. Jowett ve Victoria O'Donnell, *Propaganda and Persuasion*, 3. baskı, Thousand Oaks, Calif.: SAGE Publications, 1999, pp. 166–167'de atıfta bulunulmuştur.

7 Bu fikir birliği, 1970'lerde, deneklere yeni bilgiler sunulduktan sonra bile, sabit tutumların değişmeye karşı direncini gösteren bir dizi araştırmadan sonra ortaya çıktı. Araştırmacılar, “bir kez oluşturulduktan sonra izlenimlerin oldukça esnek olduğu” sonucuna vardılar; Lee D. Ross, Mark R. Lepper, Fritz Strack ve Julia Steinmetz, “Sosyal Açıklama ve Sosyal Beklenti: Gerçek ve Varsayımsal Açıklamaların Öznel Olabilirlik Üzerindeki Etkileri”, *Journal of Personality and Social Psychology*, Cilt. 35, No. 11, 1977; Charles G. Lord, Lee D. Ross, ve Mark R. Lepper, “Önyargılı Asimilasyon ve Tutum Kutuplaşması: Önceki Teorilerin Daha Sonra Düşünülen Kanıtlar Üzerindeki Etkileri”, *Kişilik ve Sosyal Psikoloji Dergisi*, Cilt. 37, No. 11, 1979. Ayrıca bkz. Pratkanis ve Aronson, 2001, s. 40-47.

ya da zihni, inancı oluşturan bilgiler hatalı olsa bile sonradan düzeltilir. ⁸ Bu bazen *inanç azmi olarak adlandırılır* ve özellikle tutum, bireyin kimliği veya sosyal konumu için önemli olduğunda telaffuz edilir. ⁹ Çok sayıda araştırma, olgusal bilgilerin sunulmasının bazen bir bireyin politika tercihlerini değiştirebileceğini, ancak tutum değişikliği konusunda yeni bilgiler sağlamanın etkinliğinin tutarlı olmadığını bulmuştur. ¹⁰ Genel olarak, bir bireyin inançlarına meydan okuyan bilgiler hoş karşılanmaz ve özellikle bu inançlara güçlü bir şekilde inanıldığında, istenmeyen bilgileri aktif olarak bastırmak gibi telafi edici tepkiler verebilir.

İkna üzerine yapılan araştırmalar, başarılı olmak için ikna edicilerin (1) hedeflenen kitleye ulaşması; (2) mesajı, hedef kitlenin anlayabileceği şekilde oluşturmak; ve (3) mesajın yolda bozulmamasını sağlayın. Bunların hepsi, mesajın bireye ulaşmadan önce, o bireyin içsel prizmaları aracılığıyla çarpıtılacağı potansiyel sosyal manipülasyon tuzaklarıdır.

Araştırmalar, belki de motive edilmiş akıl yürütmeye desteklenen sabit tutumların bile, bir dereceye kadar karşıt bilgilerle değiştirilebileceğini öne sürüyor. Bir çalışma, motive olmuş akıl yürütmelerin aktif olarak tutulan yanlış görüşleri düzeltebileceğini buldu. Ancak gereken bilgi miktarı önemlidir ve geri tepme etkisi riski devam etmektedir. Çalışma, yanlış görüşleri düzeltmeye yönelik ilk çabaların gerçekten de bir geri tepme ürettiğini buldu.

8 Brendan Nyhan ve Jason Reifler, *Yanlış Bilgilendirme ve Doğrulama: Araştırma Bulguları Social Science'dan*, Washington, DC: New America, Şubat 2012, s. 3; Rohini Ahluwa-lia, “İkna Direncinin Altında Olan Psikolojik Süreçlerin İncelenmesi”, *Dergi Tüketici Araştırmaları*, Cilt. 27, Sayı 2, 2000.

9 Bkz. Jonathan Haidt, “Twenty-First Century için Moral Psikoloji”, *Journal of Moral Eğitim*, Cilt. 42, Sayı 3, 2013; Hugo Mercier ve Dan Sperber, *Aklın Gizemi*, Cambridge, Mass.: Harvard University Press, 2017; ve Steven Sloman ve Philip Fernbach, *The Knowledge Illusion: Why We Never Think Alone*, New York: Riverhead Books, 2017.

10 Nyhan ve Reifler (2012, s. 8–10), 1990'lardan 2012'ye kadar, yeni bilgilerin sunulmasının bir bireyin belirli bir politika hakkındaki görüşünü değiştirip değiştiremeyeceğini ölçen birkaç çalışmaya genel bir bakış sunar. Önemli değişkenler, bir kişinin dünya görüşü için politika pozisyonunun önemini, bu pozisyona veya politikaya ne kadar güçlü inandıklarını ve yeni bilgiyi sağlayan kaynağı içerir. Bu, bir sonraki bölümde daha ayrıntılı olarak tartışılacaktır.

alınan toplam bilginin yaklaşık yüzde 15'ine kadar devam eden bu görüşleri güçlendirmenin etkisi, akıl yürütenin inançlarına ters düşüyordu. Ancak bu noktadaki etki sadece dengelendi: Motive olmuş akıl sahipleri, mevcut bilgilerin yaklaşık yüzde 30'u aksi yönde koşana kadar taahhütlerini aktif olarak sorgulamaya başlamadılar.¹¹

Yine de düşmanca sosyal manipülasyonun her zaman yerleşik tutumlara karşı gelmesi gerekmez. Alıcı nüfus belirli bir konu hakkında sabit tutumlara sahip değilse - örneğin Kuzey Atlantik Antlaşması Örgütü'nün (NATO) Baltık'ı savunması gerekip gerekmediği gibi - yeni bilgiler ortaya çıkan inançları sabit tutumlarla yapamayacağı şekillerde şekillendirebilir. Bu, özellikle sosyal manipulatörler, insanların sorunu gördüğü bağlamı şekillendirmek için çerçeveleme teknikleri kullanıyorsa doğrudur. Bu ayrım, tüketici ürünlerinin reklamını yapmayı amaçlayan ikna ile politik tutumları hedefleyen ikna arasındaki olası farkı netleştirmeye yardımcı olur: Belirli bir ürüne bağlılığı yöneten tutumlar, politik tutumlardan çok daha az yoğun olabilir. Öte yandan, bazı siyasi tutumlar diğerlerinden daha güçlü tutuluyor ve bu da etki için bir alan olduğunu gösteriyor.

Ayrıca, sosyal medya aracılığıyla edinilen bilgilerin tutumları değiştirmede gerçek bir etkisi olabileceğine dair gerçekten de bazı cesaret verici kanıtlar var. Pew Araştırma Merkezi'nin yakın tarihli bir anketinde, Amerikalıların yaklaşık yüzde 20'si siyasi bir konu hakkında fikrini değiştirdiğini ve yüzde 17'si siyasi bir aday hakkında fikrini değiştirdiğini iddia etti.

11 David P. Redlawsk, Andrew JW Civettini ve Karen M. Emmerson, "Duygusal Devrilme Noktası: Motive Edilmiş Akılcılar Hiç 'Anladım' mı?" *Politik Psikoloji*, Cilt. 31, No. 4, 2010, s. 583. Bu etki, insanların kendi görüşlerini eleştirel olarak değerlendirmelerine yardımcı olmaya adanmış çevrimiçi forumlarda bile kendini gösteriyor. Reddit'te 200.000'den fazla üyeden oluşan ve kullanıcıların fikirlerini sunmalarına ve başkalarını fikirlerini değiştirmeye davet etmelerine olanak tanıyan çevrimiçi bir forum olan ChangeMyView'deki binlerce tartışma başlığını analiz eden yakın tarihli bir araştırma, ChangeMyView platformunu kullanmanın araştırmacılara şu fırsatı verdiğini buldu: Başkalarının tartışmalı siyasi ve sosyal konulardaki sabit (ve muhtemelen güçlü bir şekilde tutulan) tutumlarını değiştirmeye yönelik gerçek yaşam girişimlerini gözlemleyin. Araştırmacılar, bu topluluğun nispeten açık fikirli insanlardan oluşmasına rağmen (bu foruma katılmayı seçmeleriyle kanıtlanmıştır), vakaların çoğunda (yüzde 70) başlangıçta sahip olunan fikirlerin değişmediğini; Chenhao Tan, Vlad Niculae, Cristian Danescu-Niculescu-Mizil ve Lilian Lee, "Winning Arguments: Interaction Dynamics and Persuasion Strategies in Good-Faith Online Discussions," *25th International World Wide Web Conference, Conference Proceedings*, Montreal, Kanada: Uluslararası World Wide Web Konferansları Yönlendirme Komitesi, Nisan 2016.

sosyal medyada gördükleri bir şey yüzünden. "Hala", anketle ilgili bir rapor sonuçlandı,

Sosyal medya kullanıcılarının çoğunluğunun ağlarında gördüklerinin etkisinde olmadığını belirtmek önemlidir. Sosyal medya kullanıcılarının yaklaşık yüzde 82'si, sosyal medyada gördükleri bir şey yüzünden belirli bir aday hakkındaki görüşlerini asla değiştirmediklerini ve yüzde 79'u sosyal veya politik bir konudaki görüşlerini asla değiştirmediklerini söylüyor. ¹²

Vatandaşların yüzde 10'unda bile bir değişime neden olmak dramatik siyasi sonuçlar doğurabilir. Rakamlar doğruysa, diğer birçok çalışmanın önerdiğinden daha fazla etki potansiyeli önerebilirler.

Tutumlar Değiştiğinde: Tutum Değişimi Kriterleri

Sabit tutumlar değişime dirençli olsa da, araştırmalar yeni bilgilerin aşağıda özetlenen çeşitli koşullar altında bireyin tutumları üzerinde daha büyük bir etkiye sahip olabileceğini göstermiştir. Bu faktörler, modern ikna teorisinin çoğunun temelini oluşturur. ¹³ Bunlar, aslında, duyarlılık kriterleridir, yani dinleyicilerin aldıkları mesajlara en duyarlı olacağı zamanlar.

Tutumlar değiştiğinde, konuya, bağlama ve tutum değişikliğinin temeline bağlı olarak bu değişiklik geçici veya kalıcı olabilir. Mevcut araştırmalar, bilginin tutumları ve daha sonra, bazı durumlarda, aşağıdaki bölümlerde özetlenen birkaç özel durumdaki davranışı etkilemesinin daha olası olduğunu göstermektedir.

¹² Duggan ve Smith, 2016, s. 18–19.

¹³ Pratkanis ve Aronson, 2001, s. 51, temel kuralları, önceden zemini kurarak ikna çalışmalarını ("ön ikna"), güvenilir kaynakları kullanarak, zorlayıcı bir anlatı veya mesaj geliştirerek ve akıl yürütme kadar veya akıl yürütme yerine duyguları hedef alarak özetler. Ayrıca bkz. Jowett ve O'Donnell, 1999, s. 164–168.

Bilgi Tekrarlandığında

İnsanlar, bilgiye tekrar tekrar maruz kaldıktan sonra (genellikle *yanıltıcı doğruluk etkisi* veya *frekans-geçerlilik ilişkisi* olarak bilinir) *bilginin doğru olduğuna inanma eğilimine* sahiptir. kolayca temin edilebilir. ¹⁴ Tanıdık mesajlar genellikle tanıdık olmayan mesajlara göre daha az incelemeye tabi tutulur. ¹⁵ Hatta bir araştırma, aynı görüşü aynı kişiden birden çok kez duymanın, bunun yaygın olarak kabul edilen bir görüş olduğu gibi yanlış bir izlenime yol açabileceğini ve bu da insanları bu görüşe daha açık hale getirdiğini buldu. ¹⁶

Bilgi Birden Fazla Kaynaktan Geldiğinde

Bilgiler, gerçekler veya iddialar, birden fazla kaynak tarafından yeniden ifade edildiğinde daha güçlü görünür. Sosyal bilim araştırması, "[p]insanlar, birden fazla kaynaktan gelen bilgilerin muhtemelen farklı bakış açılarına dayandığını ve bu nedenle daha fazla dikkate alınmaya değer olduğunu varsayıyor" diyor. ¹⁷ Birden çok kaynağın katılımının, alıcının bilginin doğru olması gerektiği yönündeki sağduyulu tepkisini ileteceği mantıklıdır. Bu tepki, aynı partizan veya ideolojik iknanın birden fazla kaynağının bir mesajın görünürdeki geçerliliğini pekiştirmek için birlikte çalıştığı yankı odaları içinde bile doğru olabilir.

¹⁴ Nyhan ve Reifler, 2012, s. 16. Ian Skurnik, Carolyn Yoon, Denise C. Park ve Norbert Schwarz, "Yanlış İddialara İlişkin Uyarılar Nasıl Öneriler Olur", *Journal of Tüketici Araştırması*, Cilt. 31, No. 4, 2005. Yanıltıcı gerçek etkisinin etkisi hem politik hem de tüketici davranışlarında belgelenmiştir. Başlangıçta, etkinin yalnızca bireylerin bir konu veya ifade hakkında oldukça belirsiz olduklarında meydana geldiğine inanılırken, aynı çalışma, bir ifadenin tekrarının bilişsel olarak işlemeyi kolaylaştırdığını ve bu da insanlar hakkında bilgili olsalar bile daha makul görünmesini sağladığını göstermiştir. bir konu; Lisa K. Fazio, Nadia M. Brashier, B. Keith Payne ve Elizabeth J. Marsh, "Bilgi, Hayali Gerçeğe Karşı Korumaz", *Journal of Experimental Psychology*, Cilt. 144, Sayı 5, 2015.

¹⁵ Matt Chessen, "Hesaplamalı Propagandanın Arkasındaki Psikolojiyi Anlamak", Shawn Powers ve Markos Kounalakis, editörler, *Kamu Diplomasisi İnternette Kurtulabilir mi?* Washington, DC: ABD Kamu Diplomasisi Danışma Komisyonu, 2017a, s. 21.

¹⁶ Kimberlee Weaver, Stephen M. Garcia, Norbert Schwarz ve Dale T. Miller, "Bir Görüşün Popürlüğünü Tanıdıklığından Çıkarsama: Tekrarlayan Bir Ses Bir Koro Gibi Seslendirebilir," *Kişilik ve Sosyal Psikoloji Dergisi*, Cilt. 92, No. 5, 2007.

¹⁷ Paul ve Matthews, 2016, s. 3.

Bir Bireyin Sosyal Grubunun Diğer Üyeleri ¹⁸ Anlayış Gösterdiğinde

İnsanlar, kendileriyle karşılaştırılabilir kişilerin de aynı şekilde inandıklarını veya hareket ettiklerini algıladıklarında, belirli bir şekilde inanmanın veya hareket etmenin uygun olduğunu değerlendirirler. ¹⁹ Çevrimiçi siyasi mobilizasyon mesajlarının davranışı nasıl etkilediğine ilişkin 2012 tarihli bir araştırma, bir kişinin Facebook ağından gelen sosyal “ipuçları” içeren mesajların yalnızca bilgi içeren mesajlardan daha etkili olduğunu buldu. ²⁰ Diğer araştırmalar, şehir efsanelerinin, hayatta kalmayla ilgili bilgiler içerdiklerinde bile, sosyal olarak anlamlı bilgiler içerdiğinde daha kolay aktarıldığını bulmuştur. ²¹

Daha geniş anlamda, sosyal bilim araştırmalarındaki en belirgin ilgili etkilerden biri *sosyal kanıt etkisidir* : insanların akran gruplarından daha fazla etkilendiği fikri. Bu etki, sosyal ipuçlarını başkalarının davranışlarını gözlemleyerek öğrenmenin, onları bireysel deneyimlerle yeniden yaratmaktan daha ekonomik olduğu gerçeğine dayanmaktadır. Sonuç, grup etkisi, konformizm ve sosyal ipucunun güçlü bir etkisidir. Bu fenomenin bir anlamı, insanların benzer inançlara sahip gruplara maruz kalma yoluyla görüşlerinde daha aşırı olma eğiliminde olmalarıdır. Sürekli bir pekiştirici görüş diyeti, insanları inanç yelpazesi boyunca daha kutuplaşmış ve aşırı pozisyonlara taşıma eğilimindedir. Viral yayılma üzerine yapılan araştırmalar, bu tür sosyal kanıt etkilerinin baskın bir açıklayıcı değişken olduğunu göstermektedir. Facebook'taki "oylamadan çık" mesajlarıyla ilgili bir araştırma, etkinliğin

¹⁸ *Sosyal grup* , kişinin sanal ağını ve fiziksel sosyal grubunu içerebilir; sosyal grup olabilir ayrıca kişinin siyasi partisi anlamına gelecek şekilde genişletilebilir. “Sosyal kanıt”ın önemine ilişkin bu noktada, örneğin bkz. Flynn, Nyhan ve Reifler, 2017, s. 136.

¹⁹ Robert Cialdini, *Pre-Suasion: A Revolutionary Way to Influence and Persuade* , New York: Simon and Schuster, 2016, s. 192–208.

²⁰ Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam DI Kramer, Cameron Marlow, Jaime E. Settle ve James H. Fowler, “A 61-Million-Person Experiment in Social Influence and Political Mobilization,” *Nature* , Cilt. 489, 2012.

²¹ Joseph M. Stubbersfield, Jamshid J. Tehrani ve Emma G. Flynn, "Seri Katiller, Örümcekler ve Siber Seks: Kentsel Efsanelerin Aktarımında Sosyal ve Hayatta Kalma Bilgisi Önyargısı", *İngiliz Psikoloji Dergisi* , Cilt. 106, Sayı 2, 2015.

Daha önce oy vermiş olan arkadaşların resimleriyle eşleştirildiğinde önemli ölçüde arttı. ²²

Gelen Bilgiler Bireyin Önceden Var Olan İnançları ve Dünya Görüşü ile Uyuştığında

Doğrulama yanlılığı ve güdülenmiş akıl yürütme ile yakından ilişkili psikolojik teorilere göre, insanların yeni bilgilere ilişkin değerlendirmeleri inançları, umutları ve korkuları tarafından şekillendirilir. İnsanlar, var olan görüşlerini doğrulayan bilgi ve argümanları aramaya veya tercih etmeye ve onaylamayanları eleştirmeye eğilimlidirler. ²³ Gelen bilgiler insanların inanmak *istedikleriyle uyumlu* olduğunda, buna inanma olasılıkları daha yüksektir. ²⁴ İnsanlar, örneğin bilimsel kanıtları, önceden var olan görüşleriyle tutarlı olduğunda daha ikna edici olarak yorumlarlar. ²⁵ Bazı

²² Bu dinamikler Alex Pentland, *Social Physics: How Good Ideas Spread- Yeni Bir Bilimden Dersler*, New York: Penguin Press, 2014, s. 50–61, 64–65.

²³ Lord, Ross ve Lepper, 1979; Kari Edwards ve Edward E. Smith, “Argümanların Değerlendirilmesinde Bir Doğrulama Önyargısı”, *Journal of Personality and Social Psychology*, Cilt. 71, No. 1, 1996; Charles S. Taber ve Milton Lodge, “Siyasi İnançların Değerlendirilmesinde Motive Edilmiş Şüphencilik”, *Amerikan Siyaset Bilimi Dergisi*, Cilt. 50, No. 3, 2006; Stephan Lewandowsky, Ullrich KH Ecker, Colleen M. Seifert, Norbert Schwarz ve John Cook, “Yanlış Bilgi ve Düzeltilmesi: Devam Eden Etki ve Başarılı Önyargılardan Kurtulma,” *Kamu Yararına Psikolojik Bilim*, Cilt. 13, Sayı 3, 2012, s. 112; Brendan Nyhan ve Jason Reifler, “The Roles of Information Deficits and Identity Threat in the Prevalence of Misperceptions,” *Seçimler, Kamuoyu ve Partiler Dergisi*, 2018. 2005 ve 2006 yıllarında yapılan bir dizi araştırma, yanlış bilgilendirilen insanlara haberlerde düzeltmeler sunulduğunu ortaya çıkardı. siyasi eğilimleriyle çelişen, nadiren fikirlerini değiştirdiler. Aslında, çoğu zaman inançlarına daha da güçlü bir şekilde bağlı hale geldiler (Nyhan ve Reifler, 2012, s. 10). Benzer bir 2007 araştırması, yanlış yönlendirilen insanlara ABD nüfusu içindeki göçmenlerin oranı hakkında doğru bilgi vermenin onların göçmenlik hakkındaki görüşlerini etkileyip etkilemeyeceğini incelemiştir. Yapmadım. John Sides ve Jack Citrin'e Bakın, *Huddled Ne Kadar Büyük Kitleler mi? Kamuoyunda Göçmen Nüfusa İlişkin Yanlış Algıların Nedenleri ve Sonuçları*, Midwest Siyaset Bilimi Derneği'nin 65. Yıllık Ulusal Konferansı'nda sunulan bildiri, Chicago, 2007.

²⁴ Nyhan ve Reifler, 2012.

²⁵ Geoffrey D. Munro ve Peter H. Ditto, “Önyargılı Asimilasyon, Tutum Kutuplaşması ve Stereotiple İlgili Bilimsel Bilgiye Tepkilerde Etki”, *Kişilik ve Sosyal Psikoloji Bülteni*, Cilt. 23, No. 6, 1997. Paul Lazarsfeld ve meslektaşlarının bulduğu gibi ABD seçmenlerine ilişkin değerlendirmelerinde, insanlar genellikle fikir oluştururken önceden var olan fikirlerini pekiştiren kanaat önderleri ararlar. Yazarların sözleriyle, “maruz kalma her zaman seçicidir;

Araştırmalar, doğrulama yanlılığının fizyolojik bir bileşeni olduğunu öne sürüyor: İnsanlar, inançlarını destekleyen bilgileri işlerken bir dopamin hücumu yaşarlar, ²⁶ ve bir çalışma, yerleşik inançların aksine bilgiyi reddetmede belirli sinirsel mekanizmaların rol oynadığını öne sürer. ²⁷ İlginc bir şekilde, bu etki, iyi bilgilendirilmiş olmakla güvenilir bir şekilde ortadan kaldırılmaz: Bazı araştırmalar, aslında, yerleşik inançlarına en sıkı şekilde tutunan belirli bir konu hakkında en iyi bilgilendirilmiş kişilerin *aslında* olduğunu göstermiştir. ²⁸ Bir noktada, motive olmuş akıl yürütmeye uğraşan kişilerin bile belirli bir konuya yönelik tutumlarını gözden geçirmeleri gereken yeterince zıt bilgiyle yüzleştiğine dair kanıtlar vardır, ancak bu eşik çok yüksek olabilir. ²⁹

Bilgi, Spesifik Hikayeye Tutarlılık ve İkna Edicilik Sağlayan Mevcut, Daha Geniş Bir Anlatıya Yerleştirildiğinde ³⁰

İnsanlar olayları anlamlandırmak için çerçeveler ararlar ve bir dizi gelişmeyi nedensel bir mantıkla bağlayan genel anlatılar bu ihtiyacı karşılamının bir yolunu sağlar. Bireysel gerçekler bu tür anlatıların kapsamı dışında sunulduğunda, daha az yapışkanlık gösterirler.

... insanların görüşleri ile dinlemeyi veya okumayı seçtikleri şeyler arasında pozitif bir ilişki vardır; Paul Lazarsfeld, Bernard Berelson ve Hazel Gaudet, *Halkın Seçimi: Nasıl Seçmen Bir Başkanlık Kampanyasında Kararını Veriyor*, New York: Duell, Sloan ve Pearce, 1948; Jowett ve O'Donnell, 1999, s. 172. Frank Biocca, "İzleyicilerin Siyasal Mesajların Zihinsel Modelleri: Televizyonun Anlamsal İşlemesinin Teorisine Doğru", Frank Biocca, ed., *Televizyon ve Siyasal Reklamcılık*, Cilt. I: *Psikolojik Süreçler*, Hillsdale, NJ: Lawrence Erlbaum Associates, 1991, s. 29; George C. Edwards III, *On Deaf Ears: The Limits of the Bully Pulpit*, New Haven, Conn.: Yale University Press, 2006, s. 208.

²⁶ Jack Gorman ve Sara Gorman, *Mezarı İnkâr Etmek: Neden Olacak Gerçekleri Görmekten Geliyoruz? Bizi Kurtarın*, New York: Oxford University Press, 2016.

²⁷ Jonas T. Kaplan, Sarah I. Gimbel ve Sam Harris, "Kişinin Siyasal İnançlarını Karşı Kanıt Karşısında Sürdürmenin Sinirsel Bağlantıları," *Bilimsel Raporlar*, Cilt. 6, Madde 39589, 2016.

²⁸ John M. Carey, Brendan Nyhan, Benjamin Valentino ve Mingnan Liu, "Gerçeklerin Şişirilmiş Görünümü? Tercihler ve Eğilimler, Deflategate Skandalı Hakkında Komplö İnançlarını Nasıl Şekillendiriyor," *Research and Politics*, Cilt. 3, Sayı 3, Temmuz-Eylül 2016.

²⁹ Redlawsk, Civettini ve Emmerson, 2010.

³⁰ Lewandowsky ve diğerleri, 2012, s. 112-113.

güç. Bununla birlikte, bu tür anlatıları belirli yanlış bilgiler için yapı iskelesi olarak kullanmak, özellikle bu tür anlatılar insanların önceden var olan inançlarıyla örtüştüğünde oldukça etkili olabilir.

Birey Kendini Güvende, Kontrolde Hissettiğinde ve Tehdit Edilmediğinde

İnsanlar kendilerini ne kadar tehdit altında veya savunmasız hissederlerse, yeni bilgilere o kadar az açık olurlar. ³¹ *Tehdit* , kişinin kimliğine yönelik algılanan bir tehdide (soyut) veya kişinin refahına yönelik algılanan bir tehdide (somut - örneğin, mültecilerin oluşturduğu bir tehdidi algılamak) atıfta bulunabilir. Bir araştırmaya göre, belirli bir tutuma meydan okumanın bireyin kimliğine yönelik algılanan tehdit ne kadar büyükse, bireyin konumunu ikiye katlama ve hatta meydan okunan inancı “din dinine çevirme” olasılığı o kadar fazladır. ³² İnsanlar kendilerini ne kadar az tehdit edilmiş veya saldırıya uğramış hissederlerse, yeni bilgilere o kadar açık olacaklardır. Yine de diğer araştırmalar, insanların bir durum üzerinde kontrol eksikliği hissettiklerinde, korkularını besleyen ve bir açıklama sağlayan bilgilere daha açık olmayı içerebilecek “yanlış algılamaların daha fazla kabul edilmesine yol açan stratejilerle telafi edebileceklerini” gösteriyor. bunun için, bu açıklama tuhaf olsa bile. ³³ Gerçekten de, korkunun özellikle tutum değişikliğinin güçlü bir katalizörü olduğuna dair güçlü araştırmalar var. ³⁴

³¹ Nyhan ve Reifler, 2018.

³² David Gal ve Derek D. Rucker, “Şüphe Halindeyken Bağırın! Şüphenin Proselize Etme Üzerindeki Paradoksal Etkileri, *Psikoloji Bilimi* , Cilt. 21, No. 11, 2010, s. 1701-1707. Ayrıca bkz. Nyhan ve Reifler, 2012, s. 11.

³³ Nyhan ve Reifler, 2012, s. 17. 2008'de *Science dergisinde yayınlanan bir makalede* , iki yönetim profesörü, katılımcılarda kontrol eksikliği yaratmanın, komplo teorilerinin varlığını algılamak da dahil olmak üzere, hiçbir şeyin olmadığı kalıpları görme eğilimlerini artırdığını buldu; Jennifer Whitson ve Adam Galinsky, “Kontrol Eksikliği Hayali Model Algısını Artırıyor,” *Science*, Cilt. 322, No. 5898, 2008.

³⁴ Witte (1992) tarafından yürütülen araştırma, korku çağrılarının en ikna edici olduğu belirli koşulları belirledi. Korkunun ikna edici olması için, hem izleyicilere tehdit edici bilgileri iletmeleri hem de tehdidi azaltmak veya ortadan kaldırmak için bir yol önermeleri gerektiğini buldu; Kim Witte, “Korkuyu Korku Temyizlerine Geri Getirmek: Genişletilmiş Paralel Süreç Modeli,” *Communication Monographs* , Cilt. 59, No. 4, 1992, atıfta bulunulan Jowett ve O'Donnell, 1999, s. 174. Mike Allen ile daha sonraki çalışmasında Witte, “güçlü korku çekicilikleri ve yüksek etkili mesajların en büyük sonuçları ürettiğini buldu.

Birey Bilgi Sağlayan Kaynağa Güvendiğinde ve Güvenilir Olduğunu Aldığında

Kaynak güvenilirliği, yeni bilgilere açıklığın belirlenmesinde önemli bir faktördür. ³⁵ İnsanlar bir hikayeyi doğrudan değerlendirmek yerine genellikle güveni bir kestirme yol olarak kullanırlar ve inanılır birinin ona inanıp inanmadığına bakarlar. Bilgilerindeki boşlukları doldurmak için o kişinin yargısına güvenirler. ³⁶ İlgili bir anlamda, bilgi, insanların kendilerine benzer olarak algıladıkları birinden geldiğinde, buna inanma olasılıkları daha yüksektir (bu argüman, psikolojik kavram olan *örtük kavramı kullanır*. insanların bilinçsiz bir tercihi olduğunu iddia eden *egotizm* kendimizle ilişkilendirdiğimiz şeyler). ³⁷

Olumsuz Bilgi ve Dil Kullanıldığında

İlginç bir şekilde, birden fazla çalışma, olumsuz bilgi ve dilin, olumlu bilgi ve dilden daha ikna edici ve daha kalıcı güce sahip olduğunu gösteriyor gibi görünüyor. gösteren kanıtlar var

davranış değişikliği, düşük etkili mesajlarla güçlü korku çekiciliği, en yüksek düzeyde savunma tepkileri üretir. Bakınız Kim Witte ve Mike Allen, “A Meta-Analysis of Fear Temyizleri: Etkileri Etkili Halk Sağlığı Kampanyaları,” *Health Education and Behavior*, Cilt. 27, No. 5, 2000, s. 591.

³⁵ Pratkanis ve Aronson, 2001, s. 121–153.

³⁶ James Druckman, “Çerçeveleme Etkilerinin Sınırları Üzerine: Kim Çerçeveleyebilir?” *Politika Dergisi*, Cilt. 63, No. 4, 2001; Lewandowsky ve diğerleri, 2012, s. 113. Etkiyi inceleyen bir çalışmada bir tüketicinin bir reklamın iddiasına inanacağı ihtimaline dayanan mesajın kaynağı, bir kaynağın güvenilirliği, ikna etme yeteneği ile ilişkilidir; Shailendra Pratap Jain ve Steven S. Posavac, “Ön Satın Alma Özelliği Doğrulanabilirliği, Kaynak Güvenilirliği ve İkna,” *Tüketici Psikolojisi Dergisi*, Cilt. 11, No. 3, 2001. Tüketicilerin inanma olasılığı daha yüksekti kaynağın güvenilir olarak görülüp görülmediğini veya ürünle ilgili deneyimi olup olmadığını iddia eder. Anketler, endişe verici sayıda Amerikalı’nın, bu teori yıllar önce gözden düşmüş olsa da, aşılardan tehlikeli olduğuna hala inandığını gösteriyor (Nyhan ve Reifler, 2012, s. 7).

³⁷ Chessen, 2017a. Hatta ismi telaffuzu kolay olan birinden gelen bilgilere (bilgiyi tüketen kişiye göre) birinin inanma olasılığının daha yüksek olduğunu destekleyen araştırmalar bile var; Eryn J. Newman, Mevagh Sanson, Emily K. Miller, Adele Quigley-McBride, Jeffrey L. Foster, Daniel M. Bernstein ve Maryanne Garry, “Adları Telaffuzu Kolay İnsanlar, İddiaların Doğruluğunu Destekliyor,” *PLOS One*, Cilt. 9, Sayı 2, 2014; ve insanların fiziksel olarak çekici buldukları biri tarafından bir pozisyonu benimsemeye ikna edilme olasılıklarının daha yüksek olduğu; Alice H. Eagly ve Shelly Chaiken, “İletişimci Özelliklerin Fikir Değişimi Üzerindeki Etkisine İlişkin Bir İlişkilendirme Analizi: İletişimci Çekicilik Örneği”, *Journal of Personality and Social Psychology*, Cilt. 32, No. 1, 1975.

İnanç azmi ve inanç yankıları olumsuz bilgilerle daha güçlüdür. ³⁸ Bu bulguların bazılarının olası bir yorumu, yanlış bilgilendirme kampanyalarındaki kritik bir dinamiğin, *önceden uyarı ile ilk hamle avantajı arasındaki ilişki olduğudur* . eğer defans oyuncusu yeterli sayıda insanı doğru önleyici teknikler ve bilgilerle aşılayabilir, bilgi saldırganını yerinden etmesi çok zor hale gelen bir anlatı yerleştirme yeteneğinden mahrum edebilir. Merkezi bir bulgu, sosyal bağlantıların önemli olduğudur: İnsanlar, bazı soyut bilgilere güvenmek yerine , *güvenilir kaynaklardan gelen bilgilere güveneceklerdir*. doğruluk veya “gerçek” kavramı. Örneğin bir Nielsen anketi, resmi medya kurumlarına güvenin azaldığını gösteren diğer çalışmalarla karşılaştırıldığında, çevrimiçi kullanıcıların yüzde 83'ünün aile ve arkadaşlardan gelen önerilere güvendiğini buldu. ³⁹

Bu araştırma, düşmanca sosyal manipülasyonun faydası için birkaç temel sonuç önerecektir. Bu tür kampanyalar, onları değiştirmeye çalışmak yerine yerleşik inançlar içinde çalışarak, örneğin güçlü görüşlere sahip kişilerin aşırı eylemlerini ateşleyerek daha etkili olacaktır. Güvenilirliğin temeli olarak sosyal kanıtı kullanabilirlerse daha etkili olacaklardır. Anlaşılması kolay, grafik tabanlı bilgi sunumları kullanırlarsa başarılı olacaklardır. ⁴⁰ Ve mesajlarını ne kadar çok tekrar edebilirlerse veya iddia edilen gerçekleri o kadar çok tekrarlayabilirler ve tekrar yoluyla varsayılan bir inanılrlık elde ederlerse daha büyük bir başarıya sahip olacaklardır.

Dezenformasyonu Düzeltmek: Geri Tepme Etkisinin Ötesinde

Sosyal bilimlerin tutum ve tutum değişikliği analizinden bildiklerimiz, büyük ölçekli tutumları etkileme çabalarının

38 Michael D. Cobb, Brendan Nyhan ve Jason Reifler, “İnançlar Her Zaman Sebat Etmiyor: Onlar Hakkında Olumlu Bilgiler Reddedildiğinde Politik Figürler Nasıl Cezalandırılıyor,” *Politik Psikoloji*, Cilt. 34, Sayı 3, Haziran 2013; Emily Thorson, “İnanç Yankıları: Düzeltilmiş Yanlış Bilginin Kalıcı Etkileri”, *Siyasi İletişim* , Cilt. 33, Sayı 3, 2016.

39 Todd C. Helmus ve Elizabeth Bodine-Baron, “Empowering ISIS Opponents on Twitter,” Santa Monica, California: RAND Corporation, PE-227-RC, 2017, s. 2.

40 Lewandowsky, Ecker ve Cook, 2017, s. 355–356.

belirli yankı odaları içinde işleyen ve sosyal bölünmeleri alevlendirmek için mevcut inançları ve görünüşte güvenilir bilgi kaynaklarını kullanmaya çalışan daha hedefli müdahalelerden daha az etkilidir. Tutumları değiştirmedeki zorluk, yanlış bilgilendirme veya yanlış bilgilendirmeyi bir kez nüfusa kattıktan sonra düzeltme çabaları yoluyla politika defterinin diğer tarafında da geçerli olabilir.

Bu tür geçersiz inançları düzeltmek olağanüstü zor olabilir. İnsanların mevcut inançlara bağlı kaldığına dair genel sosyal bilim bulgusuyla tutarlı olan bazı araştırmalar, yanlış izlenimleri düzeltme çabalarının basitçe işe yaramadığını öne sürüyor. ⁴¹ Düzeltmeler ve birinin fikrini değiştirmeye yönelik girişimler, bazı durumlarda ters etki yapabilir ve orijinal tutuma olan güveni pekiştirebilir. ⁴² Bazı durumlarda,

41 Lewandowsky ve diğerleri, 2012, s. 113–116; Brendan Nyhan ve Jason Reifler, “Grip Aşısı Hakkındaki Mitleri Düzeltmek İşe Yarar mı? Düzeltici Bilginin Etkilerinin DeneySEL Bir Değerlendirmesi,” *Vaccine*, Cilt. 33, No. 3, 2015b; Nyhan ve Reifler, “Displacecing Misinformation About Events: An Experimental Test of Causal Connections,” *Journal of Experimental Political Science*, Cilt. 2, Sayı 1, 2015a, s. 81; ayrıca bkz. Flynn, Nyhan ve Reifler, 2017, s. 130–131.

42 Bu fenomeni destekleyecek önemli bir araştırma grubu var: Lakoff (2014), bir çerçeveyi reddettiğimizde, çerçeveyi uyandırdığımızı ve istenmeyen çağrışımları bireyin zihnine daha da yerleştirdiğimizi; George Lakoff, “Beynin Metafor Devresinin Haritalandırılması: Gündelik Akılda Metaforik Düşünce”, *Frontiers in Human Neuroscience*, Cilt. 8, Madde 958, 2014. Tormala ve Petty (2002, 2004), insanların ikna edici saldırılara direndiklerinde, ilk tutumlarından daha emin olabileceklerini gösterdiler; Zakary L. Tormala ve Richard E. Petty, “Beni Öldürmeyen Şey Beni Güçlendirir: Direnmenin Tutum Kesinliği Üzerindeki Etkileri,” *Kişisel ve Sosyal Psikoloji Dergisi*, Cilt. 83, No.6, 2002; Zakary L. Tormala ve Richard E. Petty, “Kaynak Güvenilirliği ve Tutum Kesinliği: İkna Direncinin Üst Bilişsel Analizi,” *Tüketici Psikolojisi Dergisi*, Cilt. 14, No. 4, 2004. Nyhan ve Reifler (2012) motivasyonlu akıl yürütme ve hafıza ve biliş sınırlamaları gibi faktörlerin yanı sıra ırk ve etnik köken gibi kimlik faktörlerinden dolayı düzeltmelerin başarısız olabileceğini iddia etmektedir. Bir çalışma, “önceden var olan bir inancı ikna edici bir şekilde çürüten bilgiyle karşı karşıya kaldıklarında, insanların yalnızca çok küçük bir oranının -bir araştırmaya katılanların %2’si- inançlarının yanlış olduğunu açıkça kabul ettiğini” buldu. Bunun yerine çoğu, “çürümeye karşı çıkarak bir tür motive edilmiş akıl yürütme sergiledi”. Bkz. John Cook, Ullrich KH Ecker ve Stephan Lewandowsky, “Yanlış Bilgi ve Nasıl Düzeltilir”, Robert Scott ve Stephan Kosslyn, ed., *Emerging Trends in the the Sosyal ve Davranış Bilimleri*, New York: John Wiley and Sons, 2015, s. 22. Ayrıca bkz. Tan et al., 2016. İnanç azmi, negatif bilgiler düzeltildiğinde, pozitif bilgiler düzeltildiğinden daha belirgin görünmektedir; Cobb, Nyhan ve Reifler, 2013.

buna karşı koymak için gerekli olan yanlış bilginin sonraki düzeltmeden daha etkili olduğu ortaya çıktı. ⁴³

geri tepme etkisinin gücü , önemli bir incelemeye tabi tutulmuştur. Bazı araştırmacılar orijinal çalışmaların bulgularını tekrarlayamadılar ve ilk geri tepme etkisi çalışmasına katılanlardan bazıları aslında bu etkinin genellenebilirliğini reddetti. Bir yanlış izlenimi düzeltmeye çalışmanın *her* zaman orijinal inancı güçlendirmedeği ortaya çıktı. Bu tür çabalar dar koşullarda bu etkiye sahip olabilir, ancak doğru şekilde yapıldığında geçersiz bilgileri düzeltmek mümkündür. ⁴⁴ Güdülenmiş akıl yürütme hakkındaki daha geniş gerçek, güçlü bir şekilde geçerliliğini korumaktadır: İnsanlar, aksi kanıtlar karşısında bile önceden var olan inançlara bağlı kalma eğilimindedir. Sadece bu inançları düzeltmeye çalışmak bağlılıklarını *derinleştirmez* .

Bu nedenle, daha yeni kanıtlar, bu geri tepme etkisinin belirli koşullara özgü olabileceğini ve doğru bir şekilde tasarlanırsa, gerçekleri kontrol etme ve yalan söylemenin yanlış bilgilendirmeyle mücadelede anlamlı olumlu etkileri olabileceğini düşündürmektedir. (Bir çalışma, debunking çabalarının başarısı için kritik bir kriterin, işin detayı olduğunu buldu.

Araştırmalar, hızlı bir şekilde gerçekleşen bir bilgi parçası kodlandığında, kişi yeni bir bilgi alıp fikrini değiştirse bile sonraki tutum ve muhakeme üzerinde kalıcı etkilere sahip olduğunu göstermektedir (Nyhan ve Reifler, 2012, s. 12–14). . İnsanlar, başarılı bir şekilde geri çekilse veya düzeltilse bile eski bilgilere güvenmeye devam etme eğilimindedir. Emily Thorson bu fenomeni *inanç yankıları* olarak adlandırır ve bir parça olumsuz bilgiye maruz kalmanın tutumları nasıl etkilediğini gösteren birkaç çalışma yürütmüştür, hemen bir düzeltme sağlanmış olsa bile, kişi bu düzeltmeyi tamamen kabul etse ve o bireyin politik Eğilimler, onu bu düzeltmeye inanmak istemeye yatkın hale getirir. Thorson'un araştırması, iyi niyetli teyitçilerin "düzeltmenin yanlış bilginin tutumlar üzerindeki etkisini ortadan kaldıracağı" şeklindeki üstü kapalı varsayımına meydan okuyor ve bir bireye yönelik tamamen temelsiz suçlamaların veya eleştirinin bile "önemli itibar zararı" ile sonuçlanabileceğini öne sürüyor (Thorson, 2016, s. 476). İnançların başkanlık seçimleri üzerindeki etkileri için ayrıca bkz. Edwards, 2006.

43 Brendan Nyhan ve Jason Reifler, “Düzeltmeler Başarısız Olduğunda: Politik Yanlış Algıların Kalıcılığı,” *Politik Davranış* , Cilt. 32, Sayı 2, 2010; Lewandowsky ve diğerleri, 2012, s. 119–120.

44 Geri tepme etkisi hakkındaki tartışmanın mükemmel bir özeti, Daniel Engber, “LOL Some-thing Matters,” *Slate* , 3 Ocak 2018.

karşı mesaj. ⁴⁵) Ancak “yanlış bilgiyi düzeltme süreci karmaşık ve tam olarak anlaşılmamış” gibi görünüyor. ⁴⁶

Tutum değişikliğini gerçekleştirme çabalarının rolünü yöneten birçok kriterin bu ters yüzü, yanlış bilgilerin başarıyla tamamen değiştirilmesi için aşağıdaki gibi birkaç paralel kriter önermektedir:

- *Düzeltilmelerden önce uyarılar ve aşılar yapılmalıdır (aldatılmış olduklarına dair hedef popülasyonlara erken uyarılar)* . ⁴⁷ Araştırmalar, yanlış bilgi potansiyeli konusunda önceden uyarılmış insan gruplarının buna karşı daha tetikte olduğu ve uyarılmadığında olduğu gibi yerleşik hale gelmesine izin vermediği konusunda tutarlı görünüyor.
- *Çabanın bir karşı-anlatıya ihtiyacı var: Olaylar için ikna edici bir açıklama bağlamında düzeltici bilgiyi belirleyen nedensel bir açıklama.* ⁴⁸ Yanlış bilgilendirmeye karşı çabalar, yalnızca bireysel gerçekleri reddetmek. Bu gerçek ve yorum yarışmaları, bir anlatıyı diğerine karşı ortaya koyar. Yanıt, daha kapsamlı bir hikaye bağlamındaki bireysel iddialara itiraz etmelidir.
- *Geri çekmeler tekrarlanmalıdır* . ⁴⁹ Gerçeklerin tekrarının önemine uygun olarak, yanlış bilgilerin inkar edilmesi tutarlı ve tekrarlanmalıdır.
- *İtibar etkileri veya diğer sosyal maliyetler üstlenilmelidir* . Siyasi liderler, yanlış bilgiye bağlı kalmanın potansiyel olarak karşı karşıya kaldıklarında, bazı kanıtlar var.

⁴⁵ Man-pui Sally Chan, Christopher R. Jones, Kathleen Hall Jamieson ve Dolores Albaracin, “Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation,” *Psychological Science* , Cilt. 28, Sayı 11, 2017.

⁴⁶ Chan ve diğerleri, 2017.

⁴⁷ Cook, Ecker ve Lewandowsky, 2015, s. 6; Pratkanis ve Aronson, 2001, s. 332-334; Lewandowsky ve diğerleri, 2012, s. 116; Cook, Ecker ve Lewandowsky, 2017.

⁴⁸ Nyhan ve Reifler, 2015a, s. 83, 90; Lewandowsky ve diğerleri, 2012, s. 117-118.

⁴⁹ Cook, Ecker ve Lewandowsky, 2015, s. 6; Lewandowsky ve diğerleri, 2012, s. 116-117.

kamuoyunda muhalefet ya da “adlandırma ve utandırma” yaratmak, davranışlarını yönettiler.⁵⁰

Dezenformasyonla mücadele için önerilen bir yol, medya okuryazarlığı programlarının potansiyel değerine işaret ediyor.⁵¹ Bunlar birkaç ülkede bir miktar başarı ile kullanılmıştır. Bu tür programların optimal tasarımı ve ampirik etkileri daha fazla araştırmaya ihtiyaç duyar, ancak geri tepme etkisinin sınırlı etkisi ve bu programlarda bazı başarıların başlangıcı, halkın dezenformasyon konusundaki farkındalığını artırmanın etkili bir yanıtın parçası olabileceğini göstermektedir.

Sosyal Güveni Etkileyen Faktörler

Bu bölümün girişinde belirtildiği gibi, güven teması, bilgi toplumlarının etkilerinin ve sosyal manipülasyon riskinin anlaşılması için esastır. Düşmanca manipülasyon kampanyaları genellikle vatandaşların ontolojik güvenliğini, sosyal kurumlarına olan inançlarını ve gerçeklerin algılanan güvenilirliğini baltalamak için tasarlanmış yollarla güveni hedef alır. Sosyal bilim araştırmaları, sosyal güveni destekleyen veya zayıflatan faktörleri incelemiştir.

Literatür, her biri düşmanca sosyal manipülasyonun hedefi olabilecek farklı güven biçimlerini ayırt etme konusunda dikkatlidir. Yaygın olarak tartışılan bir biçim, tekrarlayan kamu anketleriyle ölçülen sosyal kurumlara güvendir. Başka bir biçim, bazen , kurumlara olan inancın ötesine geçen, *genelleştirilmiş kişilerarası güven olarak adlandırılır*. İnsanların toplumda yürüttükleri kişilerarası etkileşimlerde arta kalan güven derecesi. Siyasi kurumlara ve süreçlere duyulan güven bazen

50 Brendan Nyhan ve Jason Reifler, “The Effect of Fact-Checking on Elites: A Field Experiment on US State Legislators,” *American Journal of Political Science* , Cilt. 59, Sayı 3, 2015c.

51 Bu konuda büyüyen bir literatür var. Örneğin bkz. Monica Bulger ve Pat-rick Davison, *The Promises, Challenges and Futures of Media Literacy* , New York: Data and Society Research Institute, Şubat 2018; ve Jennifer Fleming, “Medya Okuryazarlığı, Haber Okuryazarlığı veya Haber Takdir? Stony Brook Üniversitesi’ndeki Haber Okuryazarlığı Programına İlişkin Bir Vaka Çalışması,” *Gazetecilik ve Kitle İletişim Eğitimi* , Cilt. 69, No. 2, 2014.

ayrı ölçülür. Bu kısa bölümde, bazı faktörler bir veya daha fazla kategoriyle diğerlerinden daha alakalı olsa da, bu çeşitli türler arasında güven düzeylerini etkileyen faktörlerle ilgileniyoruz. ⁵² Uluslar arasında sosyal güven ile ilişkili görünen bir değişken, prosedürel kurallar, kuralların ve yasaların uygulanması açısından adalettir. ve sonuçlarda algılanan adalet. Kökten adaletsiz bir gelir dağılımı bu kriteri ihlal eder. ⁵³

Diğer araştırmalar, fırsat eşitliği ve ekonomik sonuçların eşitliği gibi yakından ilişkili konuların, yüksek sosyal güven seviyeleriyle de ilişkili olduğunu öne sürüyor. ⁵⁴ Fırsat eşitliğini engelleyen yüksek düzeyde yolsuzluk, yine önemli ve artan ekonomik eşitsizlik seviyelerinde olduğu gibi, bu sosyal güven yollarına doğrudan bir saldırı teşkil edecektir. Araştırma, güven açısından bu tür durumlara yanıt vermede olası bir yakalama-22 önerir: Güven bir kez çökmeye başladığında, bir toplum, gerekli olacak algılanan adaleti desteklemek için evrenselci çözümlerin tam türünü engelleyen şekillerde parçalanır. güveni geri yükleyin.

Adalet konusuyla biraz bağlantılı olarak, insanların sosyal kurumların performansına olan güven derecesinin, onların kurumsal ve daha geniş sosyal güven seviyelerini etkilediğine dair bazı kanıtlar vardır. ⁵⁵ Yönetişim kurumlarının etkisiz olduğu algılandığında,

⁵² Kanıtlar karışık olsa da, güvenin bu çeşitli versiyonlarının bağlantılı olduğu fikri için bazı araştırma destekleri var - yani, düşük genelleştirilmiş sosyal güven, kurumlara olan düşük güven ile ilişkilidir. Bakınız Sonja Zmerli ve Ken Newton, "Social Trust and Attitudes Toward Democracy," *Public Opinion Quarterly*, Cilt. 72, No. 4, 2008. Ayrıca bkz. Chan S. Suh, Paul Y. Chang ve Yisook Lim, "Spill-Up and Spill-Over of Trust: An Extended Test of Cultural and Institutional Theories of Trust in South Korea," *Sosyolojik Forum*, Cilt. 27, Sayı 2, 2012.

⁵³ Jong-sung You, "Sosyal Güven: Adillik Homojenlikten Daha Önemlidir", *Politik Psikoloji*, Cilt. 33, No. 5, 2012.

⁵⁴ Bo Rothstein ve Eric M. Uslaner, "Herkes İçin Her Şey: Eşitlik, Yolsuzluk ve Sosyal Güven," *World Politics*, Cilt. 58, No. 1, 2005.

⁵⁵ Natalia Letki, "Sivil Ahlakın Kökenlerini Araştırmak: Güven, Sosyal Sermaye ve Kurumsal Performans," *Politik Davranış*, Cilt. 28, No. 4, 2006; Blaine G. Robbins, "Kurumsal Kalite ve Genelleştirilmiş Güven: Tekrarlı Olmayan Nedensel Model," *Sosyal Göstergeler Araştırması*, Cilt. 107, No. 2, 2012.

bu sadece insanların bu kurumlara olan inancını değil, aynı zamanda daha geniş anlamda sosyal güven derecelerini de etkileyebilir.

Sosyal bağların ve ağların doğasının güven düzeylerini etkilediği görülmektedir. Bazı araştırmalar, insanların gayri resmi sosyal temaslarının kalitesinin, geliştirilmiş sosyal güven derecelerini etkilediğini öne sürüyor. ⁵⁶ İnsanlar güvenilir bir sosyal temas duygusu sağlayan iyi gelişmiş gayri resmi ağlara sahip olduklarında, daha geniş anlamda güvenme yeteneklerine daha fazla inanç kazanırlar.

Karşılaştırmalı ve kültürler arası araştırmalar, toplumlar arasında güven düzeylerinde güçlü farklılıkların ortaya çıktığını ortaya koymaktadır. Bazı İskandinav ülkelerinde, insanların yarısından fazlası, diğer insanlara genel olarak güvenilebileceğini söyleyen anketlere yanıt verirken, bazı düşük güvenilen ülkelerde (Brezilya ve Türkiye gibi) bu rakam tek haneli rakamlara yakın seyrediyor. ⁵⁷ Diğer araştırmalar, bu farklı bölgelerden gelen göçmenlerin çocukları ve torunları arasında, bu farklı güven düzeylerinin nesiller boyunca sürebileceğini ileri sürmektedir. ⁵⁸ Bu nedenle bazı araştırmalar, sosyal güvenin kültürel veya etnik bir bileşeni olduğunu öne sürmüştür.

Bireysel bir bakış açısından, bir kişinin yaşam deneyimleri, sosyal güven dereceleri üzerinde önemli bir etkiye sahiptir. ⁵⁹ İnsanlar güvenmeyi (veya güvenmemeyi) kısmen, hem grup dışı deneyimler hem de eğitim ve ebeveynlik dersleri dahil olmak üzere deneyimlerinin birikimi yoluyla *öğrenirler*. ⁶⁰

Sosyal bilim araştırmaları ayrıca sosyal güvenin önemine dair güçlü kanıtlara ve dolayısıyla sosyal güvenin olası tehlikelerine işaret ediyor.

⁵⁶ Jennifer L. Glanville, Matthew A. Andersson ve Pamela Paxton, "Sosyal Bağlantılar Güven Yaratır mı? Yeni Boylamsal Verileri Kullanan Bir İnceleme, *Sosyal Kuvvetler*, Cilt. 92, No. 2, 2013.

⁵⁷ Rothstein ve Uslaner, 2005, s. 42.

⁵⁸ Eric M. Uslaner, "Nerede Durduğunuz, Büyükanne ve Büyükbabanızın Nerede Oturduğuna Bağlıdır: Genelleştirilmiş Güvenin Kalıtılabilirliği," *Public Opinion Quarterly*, Cilt. 72, Sayı 4, 2008.

⁵⁹ Jian Huang, Henriëtte Maassen van den Brink ve Wim Groot, "Kolej Eğitimi ve Sosyal Güven: Nedensel Mekanizmalar Üzerine Kanıtı Dayalı Bir Çalışma," *Sosyal Göstergeler Araştırma*, Cilt. 104, No. 2, 2011.

⁶⁰ Jennifer L. Glanville ve Pamela Paxton, "Güvenmeyi Nasıl Öğreniriz? Genelleştirilmiş Güven Kaynaklarının Doğrulayıcı Dörtlü Analizi," *Social Psychology Quarterly*, Cilt. 70, No. 3, 2007.

Düşmanca sosyal manipölasyon onu baltalamayı başırırsa ortaya çıkar. Yüksek düzeyde kişilerarası ve kurumsal güven, etkili yönetim, sivil katılım, ortak endişe konularında sosyal işbirliği, verimli ekonomik işlemler, daha yüksek ekonomik büyüme gibi sonuçlara katkıda bulunarak, sosyal kurumların etkinliği için temel bir yakıt gibi görünmektedir. ve daha fazlası. ⁶¹ Düşük güven durumlarında, hem ekonomik hem de politik olarak işlemlerin daha birçok detayı açıklanmalıdır. ⁶² Güvende bir azalma, bu nedenle, yoğunlaşmış bürokratikleşmeyi, düzenleyici aşırı erişimi ve politik kemikleşmeyi körükleyebilir.

genelleştirilmiş güvenin yerini alacak şekilde tasarlanmasıdır. bütün, *belirli bir* güven ile, yani yalnızca kişinin kendi grubuna güvenmesi. Genelleştirilmiş güven yerine özelleştirilmiş güvene yapılan vurgu, bilgi yankı odaları ile birleştirilmiş bir sosyal bölümlenme çağının önemli bir riski olabilir. Rusya'nın, örneğin bir anlaşmazlıkta her iki tarafa da yardım etmek için devreye girerek, Amerika Birleşik Devletleri'nde sınıf, ırk ve diğer bölünmeleri körüklemeye yönelik son zamanlardaki çabalarının çoğu, *tam* olarak özeli genelin üzerine yükseltme etkisine sahiptir. Böyle bir eğilim hızlanırsa, gelişmiş toplumlar için uzun vadeli sonuçlar ciddi olabilir.

Tutumların Doğası ve Değişen Bilgi Küresi

Bilgi tutumları, tutum değişikliği ve iktidarın rolüne ilişkin sosyal bilim araştırmalarının bu özeti, birkaç kapsayıcı tema önermektedir. Genel olarak konuşursak, temel tutum ve inançları değiştirmek zordur, özellikle de temel siyasi veya ideolojik meselelerle uğraştıklarında. İnsanların sosyal ağlarından ve diğer güvenilir kaynaklardan gelen etkiler, rastgele veya diğer güvenilir kaynaklardan gelen etkilerden daha fazla etkiye sahip olma eğilimindedir.

⁶¹ Francis Fukuyama, *Trust: The Social Virtues and the Creation of Refah*, New York: Free Press, 1995. Ayrıca bkz. Stephen Knack ve Philip Keefer, "Sosyal Sermayenin Ekonomik Getirisi Var mı? Ülkeler Arası Soruşturma," *Quarterly Journal of Economics*, Cilt. 112, No. 4, 1997.

⁶² Christian Bjørnskov ve Stefan Voigt, "Constitutional Verbosity and Social Trust," *Public Choice*, Cilt. 161, Sayı 1/2, 2014.

bilinmeyen kaynaklar. Birden çok kaynaktan sürekli olarak büyük hacimde tekrarlanan bilgiler, tek kaynakların iddialarından daha fazla etkiye sahiptir. Bilgi bir kez kabul edildikten ve içselleştirildikten sonra yerini değiştirmek zorlaşır.

Bu temaları, İkinci Bölüm'de tartışılan bilgi dünyasındaki eğilimlerin yanına yerleştirmek, birkaç potansiyel ders üretir. Yankı odalarının veya inanç silolarının rolü özellikle büyük görünmektedir: İnsanlar, kendi seçtikleri algılanan ideolojik arkadaşlar grupları içinde faaliyet gösterdiklerinde, duyduklarını eleştirmeden kabul etme olasılıkları daha yüksektir. Bu parçalanma, insanların zaman içinde silolarına daha fazla yerleştiği potansiyel bir yankı odası inançları sarmalı riskine işaret ediyor. Daha parçalı, subjektif bir bilgi ortamında, -bazı durumlarda mesajların kabulü için gerekli olan- güvenilirliğin tesis edilmesi daha zor hale gelir. Aynı zamanda, otomatik bilgi yayma teknolojileri artık bireylerin veya küçük grupların, iddialarının kabulünü artırabilecek, görünüşte birden çok kaynaktan gelen iddiaların “ateş hortumu”na ulaşmasını kolaylaştırıyor.

Bu kısa araştırma aynı zamanda sosyal güvenin rolünün yanı sıra düşmanca sosyal manipülasyonun potansiyel etkisine ve sanal toplumsal saldırganlığın onu baltalamada daha ayrıntılı ve tehlikeli pratiğine özel bir vurgu yapmaktadır. Bozulmuş bir bilgi ortamının birçok özelliği, toplumdaki aracı kurumlara olan inanç gibi, doğrudan sosyal güvenin temellerine saldırır. Bazıları, dezenformasyon yaymak için kişisel ağlardaki güvenin en güçlü olduğu alanlardan yararlanır.

Şimdi bilgi tabanlı saldırganlığın geleceğini şekillendirmeye yardımcı olacak bir teknoloji araştırmasına dönüyoruz. Rapor daha sonra, geleceği anlamak için üç temelin tümünü - gelişen bilgi küresinin özellikleri, bilginin tutumlar ve inançlarla ilişkisi ve ortaya çıkan teknolojiler - karşılaştırarak, üç senaryo şeklinde genel dersler çıkararak, bu konudaki yöntemleri betimliyor. bu eğilimlerin ortaya çıkabileceği

Gelişen Teknolojiler

Düşmanca sosyal manipülasyona yönelik mevcut yaklaşımlar ve sanal toplumsal savaş için daha ayrıntılı potansiyel dahil olmak üzere, bilgiye dayalı saldırganlığın önümüzdeki yıllarda gelişebileceğini anlamak için, teknolojiyle ilgili kilit alanlardaki eğilimleri anlamak önemlidir. bu devlet aracı. Şimdiye kadar, sosyal manipülasyon büyük ölçüde basit siber izinsiz girişlerin (tehlikeli bilgileri çalmak veya önemli ağlara erişim sağlamak için) sosyal medya reklamcılığı ve viral mesajları yaymak için botların kullanımı gibi güncel propaganda ve dezenformasyon sürümleriyle evliliğini yansıttı. Bununla birlikte, gelişmiş toplumların veriye dayalı temellerindeki ve son teknoloji AI ve VR teknolojilerindeki gelişmeler, mevcut sosyal manipülasyon tekniklerinin kapsamını giderek daha fazla genişletebilir. Bu araçların tamamı, açık toplumların işleyişinin uzaktan kesintiye uğraması gibi eşi görülmemiş bir tehlike oluşturabilir.

Tablo 4.1, bu bölümde tartışılan teknolojileri özetlemektedir. Özellikle, bu teknolojiler, Birinci Bölüm'de bahsedilen siber destekli bilgi saldırganlığının üçüncü alanını açar. Siber saldırılarla ilgili endişelerin çoğu, fiziksel hasara (örneğin kritik altyapıya) neden olan müdahalelere odaklanmıştır. Bugüne kadarki çoğu sosyal manipülasyon, bir dereceye kadar siyasi savaşla birleştirilmiş propagandanın güncellenmiş versiyonlarına, yani siyasi sonuçları şekillendirmek için doğrudan müdahaleye odaklandı. Giderek, düşmanca sosyal manipülasyon, sayısallaştırılmış toplumların bilgi temellerini hedef alabilecektir: veri tabanları, algoritmalar, ağ bağlantılı cihazlar ve yapay

Tablo 4.1**Gelişmekte Olan Sosyal Manipülasyon Teknolojileri ve Sanal Toplumsal Saldırganlık**

teknoloji	Açıklama
Hassas hedefleme etkilemek	Mesajları hedefleme teknikleri, genellikle değil her zaman sosyal medya platformları aracılığıyla, çok spesifik alt gruplar veya giderek artan bir şekilde bireyler
yapay zeka	İnsan düşüncesinin bilgisayar tabanlı simülasyonu ve davranış — bu çalışmanın amacı doğrultusunda, bilgi toplama, değerlendirme veya manipüle etme
algoritmik karar verme	Verileri işlemek ve üretmek için algoritmaların kullanımı otomatik öneriler veya kararlar
VR ve AR	Kısmi veya tam yapaylık sağlayan sistemler kullanıcılar için ortamlar
IoT	Karşılıklı bağlantı sağlayan birbirine bağlı cihazlar ağı farkındalık ve veri paylaşımı
Ses özellikli arayüzler	Kullanıcıların bilgi talep etmesine veya yönlendirmesine izin veren sistemler sesli komutlarla eylemler
Blockchain ve dağıtılmış finans sistemleri	Para alışverişi için defter tabanlı, taban sistemleri veya bilgi
Video ve ses sahtekarlığı	Son derece gerçekçi üretebilen programlar fabrikasyon video ve ses
Gözetim sistemleri	Yüz tanıma gibi teknolojiler, sosyal aktivitelerin anlık takibi

toplumun günlük işleyişine hakim olacak istihbarat programları.

Bir topluma diz çöktürme niyetiyle büyük ölçekte yürütüldüğünde, bu saldırılar kinetik, fiziksel siber savaş kategorisine girer. Ancak bu tür kampanyalar, kademeli olarak, parça parça ve herhangi bir atıfta bulunmadan ve hatta her zaman farkındalık olmadan yapıldığında, hedef toplumun istikrarını, kurumlarına olan güvenini ve halkının moralini bozabilir. Gelişen teknolojiler, sayısallaştırılmış bir toplumun karakteriyle birleştiğinde, devlet veya devlet dışı aktörler tarafından açık toplumların bozulmasına ilişkin çarpıcı yeni riskler yaratmaktadır.

Etkinin Hassas Hedeflemesi

Nispeten basit bir teknolojik ilerleme alanı, hassas pazarlama tekniklerinin daha da geliştirilmesini içerir. On yıl içinde, bu teknikler önemli ölçüde ilerleyecek ve son derece özelleştirilmiş mesajlarla belirli bireylerin çok daha tutarlı ve hedefli izolasyonunu mümkün kılacaktır. Bu teknikler öncelikle çeşitli sosyal medya platformları aracılığıyla, ancak aynı zamanda çevrimiçi davranışları cep telefonları, web tarayıcıları ve alışveriş alışkanlıkları aracılığıyla veri izleri oluşturan bireylere ulaşmanın diğer yolları aracılığıyla da kullanılacaktır.

Örneğin “nörohackleme”deki gelişmeler, gerçek zamanlı olarak zihinsel durumlarına ve duygusal eğilimlerine hitap eden pazarlama ve reklamcılık yoluyla insanları istek ve arzularını manipüle ederek hedefleyen “nöropazarlama”daki yeni yetenekleri kolaylaştıracaktır. Yüz tanıma analiz teknolojisi, birden fazla ülkedeki birkaç milyon kullanıcının duygularını ölçebilecek; duygu metrik algoritmaları, bu duyguları yüz tanıma yazılımından toplayıp yorumlayabilecektir. ¹ Yüz tanıma sistemlerine bağlı yapay ajanlar ve insanlarla sanal olarak etkileşim kurabilen algoritmalar da 2035 yılına kadar yaygın pazarlama araçları ve veri toplama mekanizmaları haline gelecek. ² Bu teknikler, hedeflenen pazarlamayı an be an güçlendirecek, günün çeşitli anlarında ve alışveriş, web’de gezinme veya telefonda konuşma gibi farklı etkinlikler sırasında insanlar.

Aktif kullanıcı girdilerini (kullanıcı tercihleri, alışkanlıkları, davranışları, gösterilen ilgi alanları ve IoT tarafından ortaya çıkarılan diğer modeller gibi) yüz ve duygusal tanıma teknolojisi ve metin konuşmalarından ve sosyal medya etkinliğinden elde edilen duygusal ipuçları ve duygularla sentezleyerek, markalar daha optimize edilmiş ve

1 Radek Silhavy, Roman Senkerik, Zuzana Kominkova Oplatkova, Zdenka Prokopova ve Petr Silhavy, ed., *Yapay Zeka Trendleri Akıllı Sistemlerde: Bildiriler Kitabı 6. Bilgisayar Bilimleri Çevrimiçi Konferansı 2017 (CSOC2017)*, Cilt. Ben, Cham, İsviçre: Springer Uluslararası Yayıncılık, 2017, s. 377.

2 Liesl Yearsley, “İnsanları Manipüle Etmek İçin Yapay Zekanın Gücü Hakkında Konuşmalıyız”, *MIT Teknoloji İncelemesi*, 5 Haziran 2017.

Bir bireyin ruh hali ile ilişkili özelliklerine (fiziksel, davranışsal veya mekansal-zamansal olabilir) hitap eden zamanında reklamlar. ³ Sonuç, yalnızca belirli sabit demografik, tutumsal veya davranışsal profillere göre çekiciliği hedefleyen değil, aynı zamanda ruh hali, insanların belirli bir zamanda nelere maruz kaldıkları, sağlık, düzey gibi değişken koşullarla çekiciliği hedefleyen bu araçların sürekli bir evrimi olacaktır. yorgunluk ve çok daha fazlası. Gelişmiş, AI güdümlü algoritmalar, istenen etkiyi yaratması en muhtemel olan belirli bir zamanda belirli kişilere ulaşmak için itirazları yönlendirmek için ultra hassas pazarlama modellerinin geliştirilmesine izin verebilir.

Yapay zeka

Yapay zeka, önümüzdeki 10 ila 15 yıl içinde, her sektörü ve özel bireylerin fiziksel ortamlarında ve siber uzaydaki günlük etkinliklerinin doğasını etkileyen, inovasyonun birincil kolaylaştırıcısı olacak. Bu özetle, tüm AI uygulamalarını açıklamaya veya incelemeye çalışmıyoruz, sadece AI'nın yeni nesil bilgi ile ilgili sosyal manipülasyonu nasıl güçlendirebileceğine dair birkaç örnek sağlamaya çalışıyoruz. Ayrıca, AI'nın büyük ekonomilere nüfuz etme derecesini veya AI'nın bir sosyal manipülatörün elinde neler başarabileceğini abartmak mümkündür; pratik, gerçek dünyadaki uygulamaları şu ana kadar yalnızca kademeli olarak geliyor. Bu nedenle, sosyal manipülasyon ve sanal toplumsal saldırganlık için çıkarımları değerlendirirken, önümüzdeki on yılda AI ilerlemelerinin veya uygulamalarının hızını abartmamak önemlidir. ⁴ Bununla birlikte, önemli olmaları muhtemeldir.

Basitçe söylemek gerekirse, AI, örüntü ve konuşma tanıma, stratejik seçim, görsel algılama gibi alanlarda, girdilere ve bilgi işlemeye verilen akıllı yanıtları simüle etmek için bilgi işlem kullanımını içerir.

³ CY Yam, "Derin Öğrenmeyi Kullanarak Metinden Duygu Algılama ve Tanıma," *Micro-soft Developer Blog*, 29 Kasım 2015.

⁴ Kısa vadeli ve uzun vadeli uygulamalar arasındaki ayrım Michael C. Horowitz, "Yapay Zeka, Uluslararası Rekabet ve Güç Dengesi", *Texas National Security Review*, Cilt. 1, Sayı 3, Mayıs 2018, s. 41-42.

ve çeviri. “Yapay zeka, makineleri akıllı hale getirmeye adanmış çalışma alanıdır. İstihbarat, bir sistemin çok çeşitli ortamlarda hedeflerine ulaşmak için en iyi hareket tarzını belirleme yeteneğini ölçer.”⁵ Makine öğrenimi, verileri değerlendirmek ve işlemek için algoritmaların veya diğer işleme talimatlarının uygulanmasıdır; burada makine performansını yineleyebilir ve çok sayıda örneği işleyerek zaman içinde geliştirmek için kalıpları ve stratejileri “öğrenebilir”.

Yapay zeka sistemleri, dama, satranç, Go ve hatta oyuncuların yalnızca eksik bilgiye sahip olduğu bir oyun olan poker gibi karmaşıklığı artan oyunlarda insanları yenmek için artan bir yetenek gösterdi. Libratus adlı ilk AI poker şampiyonu, 2017'de önde gelen insan oyuncuları yendi. AI'nın makine öğrenme potansiyeli, Go oyunu bağlamında gösterildi: İkinci nesil bir AI sistemi olan AlphaGo Zero, karşı 4,9 milyon oyun oynadı. üç günlük bir süre içinde kendini geliştirdi ve daha sonra birinci nesil program AlphaGo'yu 100 kez yenecek kadar yetkin hale geldi.⁶

Son çalışmalar, önümüzdeki on yılda yapay zekada bir dizi olası gelişmeye işaret ediyor.⁷ Bu gelişmeler, büyük veri kümelerini yalnızca tek geçişle işleyebilen veya denetimsiz işleme çabalarında veriler üzerinde çalışabilen algoritmaların kullanımını içerir. “Derin öğrenme” yoluyla geliştirilen, sinir ağlarını simüle eden makine öğrenimi süreçleri, görüntülerde ve videolarda nesne ve aktivite tanıma ve ses, konuşma ve doğal dil işlemede duyuşsal algılamadaki ilerlemeleri hızlandırdı ve hızlandırmaya devam edecek. Yapay zeka, davranışsal psikoloji ile entegre edildiğinde robotların, yapay ajanların ve programların “deneyime dayalı sıralı karar verme” yoluyla öğrenmesini sağlamaya başlayacaktır. AI uygulamaları, konuşma tanıma yeteneklerine bağlı gelişmiş doğal dil işlemeye sahiptir ve muhtemelen gelişmiş sözlü iletişimi mümkün kılacak şekilde bunu yapmaya devam edecektir.

5 Paul Scharre ve Michael C. Horowitz, *Yapay Zeka: Her Politika Yapıcı Nedir? Bilmeniz Gerekenler*, Washington, DC: Yeni Bir Amerikan Güvenliği Merkezi, Haziran 2018, s. 4.

6 Scharre ve Horowitz, 2018, s. 8.

7 Peter Stone ve diğerleri, *Yapay Zeka ve 2030'da Yaşam: Yapay Zeka Üzerine Yüz Yıl Çalışması*, Stanford, Kaliforniya: Stanford Üniversitesi, Eylül 2016, s. 14–17.

insanlar ve yapay ajanlar veya sistemler arasında ve ana akım dillerin gerçek zamanlı çevirisi.

İlgili robotik alanında, AI, robotları insancıllaştırmak ve AI, IoT ve video ve seste yeni teknolojilerin ve yeteneklerin bir sentezini içerecek olan birçok basit insan işi görevini yerine getirebilen robotik varlıklar üretmek için uzun vadeli bir itici güç sağlıyor. üretme. 20 yıl önce internetin olduğu yerde bugün de robotik ile aynı yerdeyiz. ⁸ Önümüzdeki 20 yıl içinde robotların, yaşlı bakıcı, ev hizmetleri ve ulaşım endüstrilerinin yanı sıra sınıf ve işyerindeki bazı insan çalışanları duyuşsal algılama, nesne tanıma, uzamsal akıl yürütme ve el becerisi ile yerinden etmeye başlaması muhtemeldir. bağlamsal anlayış, duygusal anlayış ve taklit yetenekleri. Bu süreç yalnızca önümüzdeki beş ila on yıl içinde başlayacak, ancak çeşitli araştırmalar 20 ila 30 yıl içinde işgücünün yarısının robotik ikamelerle yerinden edilebileceğini gösteriyor. ⁹

Daha yakın vadede, ekonomik ve sosyal bilgi işleme AI entegrasyonunun, bireylerin faaliyetlerine (hem çevrimiçi hem de çevrimiçi) dayalı olarak sosyal ve ekonomik seçimlerini ve tercihlerini ölçmek, kaydetmek, analiz etmek ve tahmin etmek için gelişmiş algoritmalara sahip otomatikleştirilmiş sistemlere izin vermesi muhtemeldir. , giyilebilir veya implante edilebilir cihazlar aracılığıyla giderek daha fazla çevrimdışı; IoT'nin artan kullanımı; gözetim ve “sousveillance” ve arkadaşlarının, iş arkadaşlarının ve ailelerinin etkinliği). Bu eğilimin ilk unsurları, büyük teknoloji şirketlerinin yapay zeka güdümlü reklam platformlarında zaten mevcut.

Şu an için yapay zeka, dağlarca mevcut veriye ve başarıyı değerlendirmek için net kriterlere sahip görevlerle en alakalı. Mevcut AI uygulamalarının birincil sınırlaması, analitik süreçlerini genelleştirememeleri, göreve ve bağlama bağımlı olmalarıdır. Özellikle süreçler derin öğrenmeyi içerdiğinde, AI için ilginç ve büyüyen bir zorluk, programcıların AI'nın yaptığı seçimleri neden yaptığından emin olamamasıdır. Bazı durumlarda, AI “oyun oynadı”

⁸ Alec Ross, *Geleceğin Endüstrileri*, New York: Simon ve Schuster, 2016, s. 28.

⁹ Darrell M. West, “Robotlar ve Yapay Zeka İşinizi Alacak mı? Otomasyonun Ekonomik ve Siyasi Sonuçları,” *Brookings Enstitüsü*, 18 Nisan 2018.

Oyunlardaki duraklamaları veya kural değişikliklerini ısrarla "kazanmaya" zorlamak gibi belirli sonuçlara ulaşmak için. ¹⁰ Yapay zeka güdümlü süreçlerin bu öngörülemeyen stratejileri, tıp teknolojisi gibi bazı alanlarda uygulanabilirliğini sınırlayabilir. Yapay zeka güdümlü bir teşhis veya tedavi süreci bu tür son çalıştırmaları deneyecek olsaydı, tehlikeli sonuçlar doğurabilirdi.

Bu ve diğer gelişmeler sayesinde AI, yüzlerce endüstri ve alanda uygulamalara sahip olacak. Sosyal manipülasyon ve sanal toplumsal saldırganlık alanlarıyla en alakalı olan şey, yapay zekanın dijital içeriğin otomatik olarak oluşturulmasına ve gerçek hayatı taklit eden yüksek doğrulukta sanal etkileşimli deneyimlere güç katabilmesinin yollarıdır. AI zaten basit karikatürler şeklinde ilkel otomatik içerik üretmeye başlıyor, ancak zamanla AI güdümlü hesaplama binlerce mesaj ve ses veya video dosyası oluşturabilecek ve sosyal medyayı bunlarla doldurabilecek.

Yapay zekanın sosyal manipülasyonla ilgili ikinci bir uygulaması, genellikle sohbet robotları veya “konuşma yapay zekası” olarak bilinen gerçekçi etkileşimli platformlardır. ¹¹ Mevcut haliyle, bu teknoloji bugün piyasada bulunan Alexa ve Siri gibi çoklu etkileşimli asistanları yönlendiriyor, ancak bunlar büyük ölçüde soru-cevap motorları olmaya devam ediyor. AI'nın, gerçek insan konuşmalarını yakından taklit edecek şekilde kullanıcılarla etkileşime girebilen ve çok düşük bir maliyetle ölçekte çoğaltılabilen sistemler oluşturabildiği ölçüde (geliştirilmekte olan bir örnek, aşağıda tartışılan Google Duplex'tir), tüm sosyal medya arena ve daha geniş bilgi küresi dönüştürülecektir. AI odaklı platformların daha geniş yetenekler geliştirmesi muhtemeldir. Yakın zamanda bir yapay zeka sistemi, insanların yaptığı argümanların parçalarını ve belirli gerçekleri bir araya getirerek argümanlara girme becerisini gösterdi. ¹² Bu tür konuşma veya etkileşimli yapay zeka, teknolojinin risklerini ortaya çıkarmaya başlar: Sosyal medyada düşmanca sohbet robotlarına ve görünüşte insan etkileşimlerine kolayca güç verebilirler. Gerçekten de, karmaşık sistem sağlama ihtiyacı gibi, yapay zekanın keskin uçlu ulusal güvenlik uygulamalarına entegrasyonunun önündeki bazı büyük engeller

¹⁰ Scharre ve Horowitz, 2018, s. 12.

¹¹ James Vlahos, “Fighting Words,” *Wired*, Mart 2018.

¹² Will Knight, “Bu Yapay Zeka Programı Sizi Bir Tartışmada Yenebilir - Ama Ne Dediğini Bilmiyor,” *MIT Technology Review*, 19 Haziran 2018b.

AI güdümlü yeteneklerin diğerleriyle entegrasyonu, bilgi uygulamaları için mevcut değildir. ¹³ Ulusal güvenlik alanında, yapay zeka, uygulanabilir hale geldikçe belirli amaçlar için kullanılan parça parça uygulanabilir.

Diğer bir bilgi tabanlı risk, çoğu dijital süreç gibi bazı AI uygulamalarının hacklenebilir olmasıdır. İki bilim adamının yakın tarihli bir makalede tartıştığı gibi, "Yapay zeka sistemlerini kasıtlı olarak altüst etmeye çalışan kötü niyetli aktörler, potansiyel olarak bu yapay zeka güvenlik sorunlarını manipüle ederek yeni bir risk kategorisi yaratabilir." Çalışma, kötü aktörlerin AI hesaplamalarının dayandığı verileri bozabileceğine veya algoritmaların takip etmesi için yeni kurallar getirebileceğine işaret ediyor; bazı durumlarda, bilgisayar korsanları, AI sisteminin görüntü veritabanlarına uyguladığı tanıma süreçlerini çarpıtan "aldatıcı görüntüler" sundu. Veya "yanlış davranışları öğrenmesine neden olan sistem verilerini besleyebilirler". ¹⁴

Algoritmik Karar Verme

Bilgisayar teknolojisinin sosyal manipülasyonla ilgili bir başka gelişmekte olan alanı, bilgiyi işlemek ve kararlar, tahminler veya tahminler yapmak için algoritmaların kullanılmasıdır. Bu tür algoritmalar, günümüzde en çok belirli arama, pazarlama ve sosyal medya platformlarında gelişmiş durumda. Temel formlarında, program belirli bir durum veya modelle karşılaştığında ne yapılması gerektiğine dair talimatları içeren basit komut dosyalarıdır. ¹⁵ Google, arama sonuçlarını önceki bilgilere göre şekillendirmek için kapsamlı algoritmalar kullanır.

¹³ Bu engellerin bir tartışması için bkz. Horowitz, 2018, s. 44. Ayrıca bkz. ML Cummings, Heather M. Roff, Kenneth Cukier, Jacob Parakilas ve Hannah Bryce, *Yapay Zeka ve Uluslararası İlişkiler: Disruption Beklenen*, Londra: Chatham House, 2018, pv

¹⁴ Scharre ve Horowitz, 2018, s. 14-15.

¹⁵ Algoritmik çözümler, AI uygulamalarının temeli olarak kullanılabilir, ancak basit algoritmalar AI değildir. Bir tanımın belirttiği gibi, "Algoritma bir dizi talimattır - bir tetikleyiciyle karşılaştığında yürütülen önceden belirlenmiş, katı, kodlanmış bir tarif. Öte yandan AI - sayısız AI uzmanlığını ve alt kümesini kapsayan son derece geniş bir terimdir - yalnızca girdilere güvenmek yerine öğrenilen girdilere ve verilere yanıt olarak algoritmalarını değiştirebilen ve yeni algoritmalar oluşturabilen bir algoritma grubudur. tetikleyiciler olarak tanımak için tasarlandı"; Kaya İsmail, "AI ve Algoritmalar: Fark Nedir?" *CMS Tel*, 26 Ekim 2018.

desenler. Amazon, müşterilerin satın almak isteyebileceği diğer ürünleri önermek için bunları kullanır.

Bununla birlikte, sosyal hayatın birçok alanında optimal sonuç kararları üretmek için algoritmalar giderek daha fazla kullanılmaktadır. Ayrıca “kimin şartlı tahliye yapacağını, kimin kredi için onaylandığını ve kimin işe alınacağını belirlemek için zaten kullanılıyorlar”.¹⁶ Frank Pasquale, birden fazla alanda algoritmik karar verme araştırmasında, internet ve bankacılık sektörlerinin bu araçları yoğun bir şekilde kullandığı sonucuna varıyor. şunu savunuyor

Çalışanların üretkenliği, web sitelerinin alaka düzeyi veya yatırımların çekiciliği hakkında vardıkları sonuçlar, bir grup mühendis tarafından tasarlanan ve bir grup avukat tarafından korunan karmaşık formüllerle belirlenir.

Pasquale basitçe "otoritenin gitgide algoritmik olarak ifade edildiği" sonucuna varıyor.¹⁷

Cathy O'Neil'in belirttiği gibi, ortaya çıkan model şudur:

davranışsal veri okyanusları. . . doğrudan yapay zeka sistemlerine beslenecek. Ve bunlar insan gözü için kara kutular olarak kalacak. . . . Bu otomatik programlar, gördüğümüz reklamları seçen, bizim için fiyatları belirleyen, dermatolog randevusu için bizi sıraya sokan veya rotalarımızı haritalayan diğer makineler tarafından nasıl tedavi edildiğimizi giderek daha fazla belirleyecek. Oldukça verimli, görünüşte keyfi ve tamamen sorumsuz olacaklar.¹⁸

Ve birçok manipülasyon biçimine karşı savunmasız olacaklar.

Böyle bir karar vermenin halihazırda başladığı bir alan etki etmek tipta vardır. Geçenlerde bir doktor, ortaya çıkan gerçeğin "hastane yatağındaki hasta sadece bir simge,

¹⁶ Will Knight, “The Dark Secret at the Heart of AI,” *MIT Technology Review* , 11 Nisan 2017. Ayrıca bkz. Kartik Hosanagar ve Vivian Jair, “We Need Transparency in Algorithms, But Too Much Can Backfire,” *Harvard Business Review* , Temmuz 25, 2018.

¹⁷ Frank Pasquale, *Kara Kutu Derneği: Parayı Kontrol Eden Gizli Algoritmalar ve Bilgi* , Cambridge, Mass.: Harvard University Press, 2015, s. 6, 8. Ayrıca bkz. Schneier, 2018, s. 82-87.

¹⁸ O'Neil, 2016, s. 173.

yatakta değil bilgisayarda olan gerçek hasta için bir yer tutucu. Bu sanal varlık tüm dikkatimizi çekiyor.” Doktorların elektronik tıbbi kayıtları incelemek için hastalarla kişisel temasta harcadıklarından iki kat daha fazla zaman harcadıklarını gösteren araştırmalardan alıntı yapıyor. ¹⁹ Zamanla, bu sistem doktorlardan bağımsız kararlar almak için algoritmaların kullanımına ilerleyecektir. New York'taki Mount Sinai Hastanesi, hasta kayıtlarındaki verileri işlemek ve hastalığı tahmin etmek için algoritmik analiz kullandı. ²⁰ Tıbbi sohbet robotları daha yaygın hale geliyor ve birçok insan, özellikle de sosyoekonomik yelpazenin alt ucundakiler ile tıp camiası arasında varsayılan arayüz olma potansiyeline sahip. ²¹

Bu araçlar çeşitli riskler taşır. Birincisi, derin öğrenme süreçleri bilgisayarların kalıpları kendi başlarına keşfetmelerine izin verdiği ölçüde, programcıları algoritmaların gerçekte nasıl çalıştığını bilmiyorlar. ²² Sonuç, "insan kaynakları, sağlık ve bankacılıkta, sadece birkaçını saymak gerekirse" algoritmik karar almanın "hızla bize yasanın gücüne çok yakın bir şey uygulayan geniş normlar oluşturmaktadır. Örneğin, bir bankanın yüksek riskli borçlu modeli size uygulanırsa, dünya size tam da böyle, bir ölü gibi davranacaktır - korkunç bir şekilde yanlış anlaşılmış olsanız bile.” ²³ İnsanlar, anlamadıkları nedenlerle kredi ve iş için reddedilecekler; daha geniş olarak, sonuçlanabilecek toplumsal kalıp bir "puan kuralı" haline gelebilir. ²⁴ Bir örnek, kişilik testlerinin şu anda “Birleşik Devletler'deki olası çalışanların yüzde 60 ila 70'inde” kullanıldığı işe alma alanıdır. ²⁵

¹⁹ Abraham Verghese, “Teknoloji Doktorları Nasıl Büro İşçilerine Dönüştürebilir?” *New York Times Dergisi*, 16 Mayıs 2018.

²⁰ Şövalye, 2017.

²¹ Douglas Cennet, “Dr. Bot Seni Şimdi Görecek,” *MIT Technology Review*, Kasım/ Aralık 2018, s. 22.

²² Şövalye, 2017.

²³ O'Neil, 2016, s. 29, 51.

²⁴ Pasquale, 2015, s. 191.

²⁵ O'Neil, 2016, s. 108.

Diğer bir büyük risk, bu araçların arkasındaki veritabanlarının yanı sıra algoritmaların kendilerinin tipik olarak tescilli olmasıdır. Şirketler, nasıl çalıştıkları hakkında mevcut bilgileri elinde tutar ve sonuçların temelini paylaşmaz. Bu ortam, adalet ve yönetim eksikliği sorunları yaratmanın yanı sıra sayısallaştırılmış, veriyle beslenen bir çağın merkezinde yer alan genel güven sorununu büyütüyor. İnsanlar, yaşamlarını etkileyen kararların gerçek temelini bilemeyecekler ve bu da artan şikayetler için bir risk oluşturuyor.²⁶

Son olarak, tüm kodlanmış bilgi süreçlerinde olduğu gibi, bu algoritmalar da en azından teorik olarak hacklenebilir. Kesintiye, hayal kırıklığına ve endişeye neden olmaya niyetli devletler veya bireyler, bir şirketin işe alım algoritmasına, bir bankanın kredi onay algoritmasına veya bir üniversitenin kabul algoritmasına girip, kurcalamanın hemen kanıtını oluşturmak için yeterli olmayacak şekilde hafifçe ince ayar yapabilir (özellikle algoritma, makine öğreniminin kısmen opak bir sonucuya), ancak rastgele ve adaletsiz görünen sonuçlar üretmek için yeterlidir. Bilgisayar korsanları, geliştirme aşamasında algoritmaları eğitmek için kullanılan verileri manipüle etmeye çalışabilir.²⁷ Halihazırda reklamcılar ve diğerleri, oyun arama motoru algoritmalarını, kalıplarını keşfederek ve bunlardan yararlanmak için materyal göndererek veya tasarlayarak dolaylı olarak denediler. Gelecekteki saldırılar çok daha doğrudan ve kötü niyetli olabilir.

Sanal ve Artırılmış Gerçeklik

Gelişen teknolojinin bir başka alanı da VR ve AR alanıdır. Her ikisinin de çeşitli biçimleri şimdi bile devreye giriyor: Örneğin, cep telefonları için, telefonun kamerasından “görülen” dünyaya çeşitli özellikler ve VR kulaklıklar için hızla hızlandırılan teknolojiler ekleyen AR uygulamaları ortaya çıkıyor. . Teknolojiler on yıllardır geliştirilmekte olsa da, bu alandaki iş dünyası liderleri ve teknoloji uzmanları arasında yapılan son anketler, bunların

²⁶ Pasquale, 2015, s. 25.

²⁷ Kira Radinsky, “Algoritmalarınız Hackerlardan Korunmuyor,” *Harvard Business Review*, 5 Ocak 2016.

ana akım haline geliyor. ²⁸ Yakın tarihli bir PwC araştırması, bir patlamanın eşiğinde bir teknoloji alanı önerdi ve 2022 yılına kadar Amerika Birleşik Devletleri'nde 55 milyondan fazla VR başlığının aktif kullanımda olacağını öngördü. ²⁹

AR ve VR'nin olası kullanımları çoktur. Çoğu, filmler, müzik ve video oyunları için daha sürükleyici deneyimler gibi saf eğlencedir. Ancak geliştiriciler, insanların ortak ağlarda çalışmasına izin vermek için VR uygulamaları üzerinde de çalışıyor; nihayetinde, iş gücünün bir kısmının sanal olarak bir çalışma ortamında “olmak” için VR kulaklıkları kullanması muhtemeldir. ³⁰ VR, tasarım amaçları için ve kapsamlı bir şekilde eğitimde kullanılabilir ve kullanıcıların hayali mekanlarda (bir ev tasarımı gibi) veya tarihi mekanlarda (antik Roma gibi) "yürümesine" izin verir.

Bu tür teknolojiler, belirli bir ürün, hizmet veya markadan ziyade bir deneyim pazarlayan, yüksek oranda hedeflenmiş yeni bir pazarlama alanını güçlendirebilir. AI, VR ve AR'de (akıllı gözlükler ve lensler gibi) yeni yeteneklerin entegre edilmesi, kullanıcılara dijital ve gerçek dünyalar arasında köprü kuran ve bir kişinin kişisel tercihlerine, ilgi alanlarına, ruh haline, çevresine ve psikolojisine göre uyarlanabilen yeni ve sürükleyici bir alan sunacak. -kal arzular. ³¹

VR ve AR'nin agresif sosyal manipülasyon potansiyeli açıktır, ancak basit olmayabilir. Çalışmalar, ortaya çıkan VR sistemlerinin saldırılara karşı savunmasız olabileceği konusunda zaten uyardı. ³² Hacker, stres yaratmak veya sonuçları çarpıtmak ve hayal kırıklığı yaratmak için tasarlanmış VR ortamlarına ek ayrıntılar ekleyebilir. ³³ Onlar

²⁸ Alex Aharanov, “Artırılmış ve Sanal Gerçekliğin Geleceği Nedir?” *Jabil Blog* , 27 Mart 2018.

²⁹ Ashley Rodriguez, “Beş Yılda VR ABD'de Netflix Kadar Büyük Olabilir,” *Quartz* , 6 Haziran 2018.

³⁰ Peter Rubin, “Sanal Gerçeklikte İşe Gideceksin,” *Wired* , Haziran 2018, s. 61.

³¹ Jayson DeMers, “Çevrimiçi Pazarlamayı Daha İyi İçin Şekillendiren 7 Yeni Teknoloji (Umarız),” *Forbes* , 15 Ağustos 2016.

³² Alfred Ng, “VR Systems Oculus Rift, HTC Vive Hacklere Karşı Savunmasız Olabilir,” *CNET* , 17 Nisan 2018.

³³ Andrew J. Andrasik, *Hacking Humans: The Evolving Paradigma with Virtual Reality* , SANS Enstitüsü, Bilgi Güvenliği Okuma Odası, Kasım 2017. Ayrıca bkz. Eric E. Sabelman ve Roger Lam, “The Real-Life Dangers of Augmented Reality,” *IEEE Spectrum* , 23 Haziran 2015.

bilinçaltında mesaj göndermenin yollarını bulabilir, kullanıcıları belirli görüşler veya kesintilerle tohumlayabilir. Genel olarak konuşursak, VR ve AR, manipülatörlerin istedikleri hedeflere ulaşmak için hackleyebilecekleri ve değiştirebilecekleri tüm sanal dünyalar sunar.

Nesnelerin interneti

IoT, evlerimizde, vücudumuzda (ve içimizde) ve fiziksel çevremizde giderek artan yoğun etkileşimli akıllı teknolojiler ağını ifade eder. On yıl içinde, yeni üretilen nesnelerin çoğu, arabalar, ev aletleri, giyilebilir cihazlar ve hatta insanlar dahil olmak üzere veri iletebilecek veya alabilecek: ilk implante edilebilir akıllı telefonun 2030 yılına kadar ticari olarak piyasaya sürülmesi ve gerçek bilgileri iletebilmesi bekleniyor. zaman biyolojik bilgilerinin yanı sıra bugün bize tanıdık gelen iletişim ve internet işlevlerini sağlar. ³⁴

IoT, insan ve makine faaliyeti, davranış, yaşam kalıpları, tercihler, iletişim, ilişkiler ve konumların her yönü hakkında bilgi sağlayan birincil veri üreticilerinden biri haline gelecek. Uygulamalar ve örnekler neredeyse sonsuzdur: buzdolapları, dolaplar, mağazalar ve üreticileri birbirine bağlayan akıllı gıda ağları; otomobiller, yayalar, hava durumu ve daha fazlasıyla ilgili sensör verilerini entegre eden akıllı şehirler; hayvancılık izleme dahil hassas tarım; termostatları, enerji şebekelerini, hava tahminlerini ve daha fazlasını birbirine bağlayan akıllı enerji yönetimi; ve imalatta endüstriyel IoT dağıtımları. İnsanlar, giyilebilir cihazlar, implante edilmiş sensörler ve konumumuz, kalp atış hızı, sıcaklık, nabız, duygusal durum ve çok daha fazlası hakkında veri tomarları besleyen çevresel sensörler ile bu ağlara giderek daha fazla bağlanacak.

Bugün geliştirilmekte olan “akıllı şehir” teknolojilerinin, kentsel ulaşım, güvenlik, güvenlik,

³⁴ Yazılım ve Toplumun Geleceğine İlişkin Küresel Gündem Konseyi, *Deep Shift: Teknoloji Devrilme Noktaları ve Sosyal Etki*, Köln, İsviçre: Dünya Ekonomik Forumu, 2015, s. 8.

enerji, halk sağlığı ve kritik altyapı. ³⁵ Akıllı ışıklar (hareket sensörleri ve alıcılarla donatılmış sokak lambaları ve trafik sinyalleri) kırmızı veya yeşil renkte açılır veya kapanır veya gecikmeleri veya sorunları IoT bağlantılı arabalara ve yayalara bildirmek için ayarlanır. Parkmetrelere ve park yerlerine bağlı benzer IoT duyuusal yetenekleri, IoT bağlantılı araçları açık alanlara karşı uyacaktır.

Akıllı araçlar, sonunda sürücüsüz arabaları içerecek, ancak tamamen sürücüsüz arabalar ve kamyonlar yaygınlaşmadan önce bile, IoT ile bağlantılı araçlar mekanik sorunları tespit edebilecek, teşhis edebilecek, rapor edebilecek ve sonunda kendi kendini onarabilecek; 911'i arayın ve kaza meydana geldiğinde acil müdahale birimlerini isteyin; sürüş süresini, rotayı ve park etmeyi optimize etmek için Küresel Konumlandırma Sistemi (GPS) özelliklerini akıllı şehir duyu sistemleri ve diğer araçlarla senkronize edin; ve bir kişinin bir sonraki hareketi veya etkinliği beklentisiyle diğer cihazları açmaları veya kapatmaları için uyararak için evde ve ofiste kişisel IoT ağlarına bağlanın. Bu arada, akıllı kameralar her yerde ve gerçek zamanlı video gözetimi ve yeni acil durum müdahale yetenekleri sağlayacaktır.

Tahminler, 2030 yılına kadar evlere giden ve evlerden gelen tüm internet trafiğinin yarısını oluşturan IoT'ye bağlı bir trilyondan fazla sensörün olacağını gösteriyor. ³⁶ IoT özellikli cihazların genel pazarı, IoT bağlantı modüllerine harcanan ek 750 milyar ABD doları ile aynı zaman diliminde 1 trilyon ABD dolarını aşabilir. Bu yoğun ağın ortaya çıkması, bant genişliğini artıran yeni ağ teknolojilerinin genişlemesini de teşvik edecektir: Sürekli ve yüksek kaliteli akış erişimi, IoT'yi desteklemek için evlerde, ofislerde ve kamusal alanlarda gerekli bir işlev ve standart teknoloji haline gelecektir. ³⁷

Bazen IoT'yi öncelikle ev veya iş yerlerindeki cihazları birbirine bağlamak olarak düşünme eğilimi vardır, ancak aynı zamanda giyilebilir veya implante edilmiş sensörleri de dahil olmak üzere insanları giderek daha fazla entegre edecektir. IoT “zihin paylaşımı teknolojileri”, insanları kendi cihazlarına ve cihazlarını diğer cihazlara bağlamak için, kolaylaştırarak ve kolaylaştırarak geliştirilmektedir.

³⁵ Codrin Arsene, “Yakında Dünyamızda 8 Şekilde Devrim Yaratacak IoT Fikirleri,” *Y Media Labs*, 24 Kasım 2016.

³⁶ Yazılım ve Toplumun Geleceğine İlişkin Küresel Gündem Konseyi, 2015, s. 7–8.

³⁷ Yazılımın ve Toplumun Geleceği Küresel Gündem Konseyi, 2015, s. 7.

veri alışverişlerini ve iletişimlerini yönetmek. Bir kişinin kan basıncı sensörü buzdolabına, akıllı tualete ve çevresel ruh hali ve stres sensörlerine bağlanacaktır; ikincisi, eğlence önerisini yönlendirmek için sanal kişisel asistanlara bağlanabilir.

Bir IoT'nin ortaya çıkışı, hem klasik siber saldırganlık hem de sosyal manipülasyon için açıkça büyük bir potansiyel taşıyor. Schneier, "her şeyin bir bilgisayara dönüşmesi" gerçeğinin doğasında var olan güvenlik açıkları hakkında yazmıştır. Amerika Birleşik Devletleri ve diğer gelişmiş ekonomilerin "ölçek ve kapsam nedeniyle temel bir değişime ulaştığını" savunuyor. . . . Her şey, birlikte çalışmasalar bile aynı ağ üzerinde oldukları ve birbirlerini etkiledikleri karmaşık hiper bağlantılı bir sistem haline geliyor." ³⁸ Saldırganların buzdolapları aracılığıyla insanların Gmail hesaplarına girmesi; ev termostatlarını kontrol eden ve konut rehinesini etkin bir şekilde tutan yazılıma eklenen fidye yazılımı; ve otelin elektronik kapı anahtarlarına erişmek için güvenli olmayan sistemlerin kullanılması. Schneier, yazılım endüstrisinin kusurlu ancak kritik bilgi güvenliği izleme, güncelleme ve yamalama özelliklerinin pratiğinin, yazılımın bir eklenti olduğu (tuvaletler, arabalar, ev güvenlik sistemleri) üreticiler tarafından takip edilmeyecek olması olduğunu açıklıyor. geleneksel yazılımlardan bile daha büyük güvenlik açıkları.

Daha aşırı saldırı biçimlerinde, saldırganlar, temsil edeceği bilgi, algılama, karar verme ve tedarik ağlarını baltalayarak IoT'nin ana bileşenlerini yıkmaya çalışabilirler. ³⁹ Ancak sosyal manipülasyonun daha incelikli biçimlerinde, devletler veya devlet dışı aktörler, sosyal sistemlere olan güveni baltalamak için çalışmanın yanı sıra yalnızca geniş kapsamlı bozulma ve verimsizlikler getirmenin yollarını arayabilir. Sensörlerdeki veya dağıtım kanallarındaki ayarları değiştirerek, insanların yanlış türde yiyecek veya ev gereçleri almasına neden olabilirler. Daha uğursuz versiyonlarda, saldırganlar tıbbi verileri değiştirebilir

³⁸ Schneier, 2018, s. 3, 7.

³⁹ Hem büyük ölçekli dijital altyapının hem de IoT saldırısının riskleri hakkında bkz. Justin Sherman ve Deb Crawford, "Securing America's Connected Infrastructure Can't Wait," *War on the Kayalar*, 4 Aralık 2018.

sistemdeki algoritmaların hastalıkları yanlış teşhis etmesi ve yanlış ilaç reçete etmesi veya tedarik etmesi için toplanıyor. Trafik düzenlerinin verimliliğini artırmak yerine azaltmak veya kazalara ve hatta ölümlere neden olmak için trafik sistemlerindeki veya otomatik arabalardaki ayarları değiştirebilirler. Dünyanın dört bir yanındaki laboratuvarlarda veya kişisel evlerde robotları araştırmak için ayarları değiştirebilir veya yıkıcı komutlar verebilirler. ⁴⁰ Saldırı örnekleri hâlihazırda sürücüsüz arabaların hacklenmesi, internet özellikli kameraların kontrolünü ele geçiren kötü amaçlı yazılımlar ve daha fazlasını içeriyor. ⁴¹

IoT, yavaş yavaş, gelişmiş toplumların temel veri toplama ve ağ iskelesini sağlayacak yoğun bir algılama, bilgi alışverişi ve karar verme ağını temsil etmeye başlıyor. Bu haliyle, sosyal kurumlara olan güveni ve inancı sarsma ve insanların daha geniş ontolojik güvenlik duygusunu bozma becerisi arayan sosyal manipülatörler için en ayrıntılı fırsatlardan birini temsil edecektir.

Ses Etkin Arayüzler

Amazon Echo (Alexa), Google Home, Apple Siri ve SONOS One gibi sesle etkinleştirilen asistanların inanılmaz büyümesi, insanların çevrelerindeki teknolojilerle etkileşim biçimini değiştiriyor. Özellikle, insan benzeri etkileşimler ve hatta konuşmalar yapabilen, giderek daha etkili hale gelen AI ile eşleştirildiğinde, sesle etkinleştirilen bu sistemler, insanların bilgi araması, çevreleyen IoT operasyonlarını yönlendirmesi ve hatta kararlar alması için varsayılan araçlar haline gelecektir. Bir anlamda diğer teknolojik kategorilerin yalnızca bir alt kümesi olsalar da, vatandaşlar ve daha geniş bilgi dünyası arasında o kadar kritik bir geçit olacaklar ki, etkileri - ve manipülasyona karşı açıkları - kendi terimleriyle anlaşılmalıdır.

⁴⁰ Will Knight, "Araştırma Robotları Eğlenmek ve Sabotaj İçin Kaçırılabilir", *MIT Technology Review*, 24 Temmuz 2018c.

⁴¹ Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Manevra ve Manip-ulate in the Digital Age*, New York: PublicAffairs, 2016, s. 99–101.

Son tahminler, sesle çalışan hoparlörlerin 2022 yılına kadar ABD'deki hanelerin yarısından fazlasına ulaşacağını ve bu tür 175 milyondan fazla konuşmacının faaliyette olduğunu gösteriyor. Ancak sesle etkinleştirilen asistanlar çoğunlukla diğer sistemlerde konuşlandırılacak: 2022 yılına kadar dünya çapında yaklaşık beş milyar bu tür yardımcı arayüz, çoğunlukla cep telefonları aracılığıyla çalışacak. Yalnızca Amerika Birleşik Devletleri'nde, bu tür asistan destekli cihazların toplam sayısının 2017 ile 2022 arasında kabaca ikiye katlanarak 870 milyona veya her Amerikalı için ikiden fazlaya ulaşması bekleniyor.⁴²

Bu tür etkileşimli sistemler, ses tanıma teknolojisine bağlıdır ve fiziksel arayüzler kadar hızlı bir şekilde gelişmektedir. Büyük bir zorluk, “doğal dili” kolayca anlayabilen sistemler geliştirmek olmuştur: İnsanların ortak fikirleri veya istekleri ifade ettikleri çoğu zaman kendine özgü yollar. Bununla birlikte, ses tanıma yazılımı artık yüzde 5'ten daha az hata oranıyla çalışabilir.⁴³

Etkileşimli motor (esas olarak, sesle etkinleştirilen bir asistanla yapılan konuşmanın diğer ucundaki ses), gerçek bir insan muhatap gibi ses çıkarma konusunda giderek daha ustalaşan, giderek daha karmaşık bir yapay zeka tarafından destekleniyor. (Bu, etkileşimli terapötik sistemler gibi gelişmiş sohbet robotlarını güçlendirmek için giderek daha fazla kullanılacak olan aynı AI uygulamaları ailesidir.) Böyle ortaya çıkan bir teknolojinin bir örneği, AI tarafından desteklenen ve güç sağlamak için geliştirilen bir doğal dil sistemi olan Google Duplex'tir. telefon ve diğer sesli etkileşimler. Randevuları ayarlamak gibi kapalı alanlarda muazzam derecede belirgin insan-sesi doğruluğu ile etkileşimli konuşmalar gerçekleştirebilir.⁴⁴

Bu tür teknolojilerin etkinliğinin katı sınırları vardır. Birkaç şirket, bir toplantı planlamak gibi görünüşte sıradan bir görevi yerine getirebilen, yapay zeka güdümlü bir sohbet robotu geliştirmeye çalışıyor.

42 Sarah Perez, “2022'ye Kadar ABD'deki Hane Halkının %55'ine Ulaşacak Ses Özellikli Akıllı Konuşmacılar”, Diyor ki Rapor, *TechCrunch* , 8 Kasım 2017. Ayrıca bkz. J. Walter Thompson Intelligence, *Speak Easy* , New York, Haziran 2017.

43 *Konuşma Tanıma Teknolojisinin Dünü, Bugünü ve Geleceği*” *Başlangıç* , 10 Ocak 2018.

44 Bakınız Yaniv Leviathan, "Google Duplex: An AI System for Real-World Tasks Over the Phone", *Google AI Blog* , 8 Mayıs 2018.

Yapay zeka insanların isteklerinin temel sağduyuyu sonuçlarını ayırt edemediği için görevin fazlasıyla zor olduğu kanıtlandı. ⁴⁵ İnsan yargıçlardan oluşan bir heyeti, gerçek bir insanla etkileşim kurduklarına inandırarak kandırabilecek bir sohbet robotu yaratmaya yönelik sürekli bir teknoloji mücadelesi, henüz özellikle başarıya yaklaşmadı. Yine de insanlar bugün var olan nispeten ilkel sohbet robotlarına bile önemli derecede duygusal bağlılık bildiriyor ve sohbet robotları zaten tıbbi ve yasal tavsiyeler veriyor ve birçok müşteri hizmetleri etkileşimine ilk giriş kapısı olarak hizmet ediyor. ⁴⁶ Teknoloji geliştikçe, temelde yeni bir etkileşimli deneyim yaratmak için sesle etkinleştirilen arayüzlerle eşleştirilecektir.

Giderek, bu sistemler insanların duygusal durumlarını algılama yeteneğini kazanıyor. Amazon, Alexa kapı görevlisinin konuşmacının duygusal durumunu anlamasını sağlamak için ses analizi yetenekleri geliştiriyor. SONOS, “[bir dinleyicinin] sesindeki duyguya veya giyilebilir bir cihazdan elde edilen ter veya kalp atış hızı gibi biyometrik verilere dayalı olarak çalma listelerini özelleştirebilen ve dinleyicinin müzik geçmişiyse çapraz referanslı bir teknoloji için patent başvurusunda bulundu”. ⁴⁷

Zamanla, bu portalların farklı bir meraklı (ve genellikle yanlış) bilgisayarlı soru-cevap teknolojileri kategorisinden insanların etraflarındaki daha büyük teknoloji sistemleriyle etkileşimlerinin çoğunu yürüttüğü temel portal haline gelmesi muhtemeldir. (Endüstri liderleri bu eğilime "ortam hesaplama"nın yaratılması olarak atıfta bulunmaya başladılar. ⁴⁸) Dönem ödevlerini dikte etmek, internet aramaları yapmak, paket servisi sipariş etmek, termostatları ayarlamak, diyet parametrelerini dikte etmek (ve marketlere gönderilen siparişler) ve tıbbi teşhisler hakkında diyaloglar gerçekleşecek.

⁴⁵ John H. Richardson, “AI Sohbet Robotları, Bizi Öfkeliendirmeden Toplantı Planlamaya Çalışıyor,” *Wired*, 24 Mayıs 2018.

⁴⁶ Örneğin, bkz. Arielle Pardes, “Kişisel Sohbet Botum Bana Yapay Zekanın Geleceği Hakkında Ne Öğretiyor,” *Wired*, 12 Kasım 2017.

⁴⁷ Nitasha Tiku, “Fotoğraflarımızı Paylaştığımız Kadar İsteyerek Duygu Durumumuzu Paylaşacağız” *Wired*, Haziran 2018, s. 55.

⁴⁸ Paul Cutsinger, “Mark Cuban: Ses, Ortam Bilişimi Gelecektir. Geliştiriciler Hemen Girmeli,” *Amazon Alexa Blog*, 25 Mart 2019.

bu portal aracılığıyla. Başka bir deyişle, insanlarla teknoloji arasındaki temel etkileşimli ortam, dijital girdiden (yazma, işaretle ve tıkla ve dokunmatik ekranlar) sözlüye geçiş sürecindedir.

Ses-etkin arayüzlerin yükselişi, düşman aktörlerin sürece müdahale etmesi ve sosyal kesintiler yaratması için birden fazla fırsat yaratacaktır. AI arayüzünü çalıştıran yazılımın etkinliğini basitçe düşürebilir ve kullanıcı tarafında hayal kırıklığı yaratabilirler. Daha kötü senaryolarda, manipülatörler (kendileri yapay zeka tarafından desteklenen ölçeklenebilir müdahalelere sahip) arayüzleri ele geçirebilir ve yanlış (basit bir bilgi sorgusuna geçersiz bir yanıt), yıkıcıya (arabirim hakkında yanlış bilgi vererek) kadar değişen yanıtlar vermelerini sağlayabilir. bir restoranın konumu), aktif olarak düşmanca davranmak (sorgulara sürekli olarak yargılayıcı veya küçümseyici yanıtlar). Sosyal manipülatörler, ortaya çıkan bu sesle etkinleştirilmiş “ortam hesaplama” ortamının kısmi kontrolünü bile kazanabildikleri ölçüde, bir toplumun yaşamlarına egemen olan teknolojilerle varsayılan etkileşimli kanallarını şekillendirebileceklerdir.

Blockchain ve Dağıtık Defter Sistemleri

Dağıtılmış defter teknolojisi, cihazların ne zaman, nasıl ve neyle veya kiminle iletişim kurduğunu, etkileşime girdiğini veya işlem yaptığını izlemek için birincil teknoloji olarak ortaya çıkacaktır. Otomatik eşler arası, cihazdan cihaza sözleşmeli davranışı etkinleştirecek ve güvenilir dijital altyapı için bir platform sağlayacaktır. 49 Blok zinciri , örneğin para (Bitcoin gibi), hisse senedi sertifikaları veya talimatlar gibi birçok değiş tokuş türünü yansıtabilen, merkezi olmayan, dağıtılmış ve karşılıklı olarak doğrulanmış bir defterdir . Amaç, “muhasebeye radikal, merkezi olmayan bir yaklaşım yoluyla güven maliyetini büyük ölçüde azaltmak ve buna bağlı olarak ekonomik organizasyonları yapılandırmak için yeni bir yol yaratmaktır”. 50

49 “Blockchain and the Internet of Things: The IoT Blockchain Opportunity and Challenge,” *i-SCOOP* , Eylül 2016 (Şubat 2018’de güncellendi).

50 Michael J. Casey ve Paul Vigna, “In Blockchain We Trust,” *MIT Technology Review* , 9 Nisan 2018.

Bitcoin gibi mevcut dijital ve kripto para birimlerindeki gerçek değer, aslında para birimi değil, tüm işlemleri merkezi olmayan düzenlemelerle kaydeden ve hiçbir merkez bankası, ulus devlet veya herhangi bir merkezi kurumsal kontrol içermeyen bir kamu defteri fikridir. ⁵¹ 2030'a kadar izlenen blok zincirleri (AI algoritmik izleme ve analiz sistemleri ile geliştirilmiş) finansal gözetim, izleme, raporlama ve gözetim için temel oluşturacaktır. 2015 yılında bilgi ve iletişim teknolojisi yöneticileri ve uzmanlarıyla yapılan bir ankete katılanların yaklaşık dörtte üçü, 2025 yılına kadar verginin “ilk kez bir hükümet tarafından bir blok zinciri aracılığıyla” toplanmasını beklediklerini söyledi. ⁵² Bu tür sistemler amaçlandığı gibi çalışırsa, paylaşılan bilgi defterlerinin sosyal manipülasyon potansiyelini azaltmaları gerekir: Yoğun kriptografi ve özellikle dağıtılmış kullanıcılar tarafından devam eden karşılıklı doğrulama nedeniyle, bilgisayar korsanlarının blok zinciri kayıtlarını değiştirmesi çok zor olmalıdır. .

Ancak blok zincir teknolojisi aynı zamanda toplumdaki ekonomik değerın giderek artan bir şekilde sanallaştırılmasına da kapı açıyor ve bu da ulusları bilgi ortamlarını dışarıdan kurcalamaya karşı çok daha savunmasız hale getirebilir. Blockchain teknolojisi, *dijital varlıklar* için potansiyel yaratır : Bitcoin gibi yalnızca dijital biçimde var olan benzersiz şekilde tanımlanabilir, kopyalanamaz varlıklar. Herhangi bir değer biçimi teorik olarak bu tür teknolojilerle dijitalleştirilebilir. Yine de programlanabilir herhangi bir şeyin hacklenebilir olduğu kuralını takip edersek, düşman sosyal manipölatörlerin kriptografiyi ve bu talimatları değiştirmek için bir blok zincirinin dağıtılmış kontrollerini geçmenin yollarını bulma potansiyeli çok ciddiye alınmalıdır.

Video ve Ses Sahtekarlığı

Gelişen teknolojinin kritik bir alanı, özellikle yanlış bilgi veya dezenformasyonun yayılmasında olmak üzere, sosyal manipülasyondaki mevcut çabaları tamamlayabilen, ses ve video üretme yeteneğidir.

⁵¹ Ross, 2017, s. 98–103; Yazılımın ve Toplumun Geleceği Küresel Gündem Konseyi, 2015, s. 24.

⁵² Yazılımın ve Toplumun Geleceği Küresel Gündem Konseyi, 2015, s. 26.

sahte olayları gerçekmiş gibi gösteren görüntüler. Bu tür teknolojilerin yeni nesil manipülasyon kampanyalarını körüklemeye potansiyelini hayal etmek kolaydır: ulusal liderlerin özel açıklamalarının dağıtılmış ses kayıtları; halkın tepkisini çekmek için tasarlanmış patlayıcı olayların videosu; veya olayların alternatif versiyonlarını sağlayarak bir saldırganın suçluluğunu ortadan kaldırmak için tasarlanmış ses ve video (Çin gemilerinin Güney Çin Denizi'nde başka bir davacının balıkçı teknesine çarpmadığını "kanıtlayan" bir video gibi). Ortalama insanların karşılaştıkları ses ve video bilgilerinde gerçek olanı icat edilenden ayırt etmesinin son derece zor olacağı bir çağın eşiğindeyiz.

Üretilmiş Ses

Bilgisayar tarafından oluşturulan ses yeni bir fenomen değildir. Çevrimiçi çevirmenlerden cep telefonlarındaki uygulamalara kadar, bir cümle oluşturmak için kısa kaydedilmiş konuşma parçaları koleksiyonunu birbirine bağlayarak bilgisayar tarafından oluşturulan ses sağlayan çok çeşitli hizmetler vardır. ⁵³

Bununla birlikte, bunun gibi dijital sesler, şu anda ezberlenen cümle parçalarıyla ve konuşmada bulunan duygu ve cümle akışı gibi doğal eğilimlerin olmamasıyla sınırlıdır, bu da genellikle sesin biraz sentetik çıkmasına neden olur. ⁵⁴ Bu sınırlama, gerçek bir kişinin sesi ile bir bilgisayar tarafından üretilen ses arasında ayırım yapmayı kolaylaştırır. Buna karşılık, şu anda geliştirilmekte olan ses üretme teknolojisi, daha doğal bir ses yaratmak amacıyla insan konuşmasının özelliklerini öğrenmek ve taklit etmek için sinir ağlarındaki son atılımları kullanarak farklı şekilde çalışıyor. ⁵⁵ Bilgisayar tarafından oluşturulan konuşmanın genel kalitesini iyileştirmeye ek olarak, herhangi bir kişinin sesini sıfırdan kopyalamak için teknoloji geliştirilmektedir; bu, herhangi birinin manipülatörlerin istediği her şeyi söylemesini sağlamak için kullanılabilir. Bu yazılımın bir örneği, 2016 yılında VoCo adlı bir yazılımın teknoloji demosunu sunan Adobe tarafından geliştirilmektedir. Sesin Photoshop'u olarak anılan yazılım

⁵³ "Sahte Haber: Henüz Hiçbir Şey Görmediniz," *The Economist* , 1 Temmuz 2017.

⁵⁴ "Sahte Haber: Henüz Hiçbir Şey Görmediniz," 2017.

⁵⁵ Avi Selk, "Bir Robotun Bu Ses Klibi, Trump Olarak Sahte İnsan Seslerinin Geleceğinin Öncüsü," *Washington Post* , 3 Mayıs 2017.

bir ses kaydından sözcükleri silme veya yeni metin girerek sözcükleri ekleme yeteneğini gösterdi; bu, daha sonra yazılımın konuşmacıyı taklit ederek oluşturduğu. ⁵⁶ Geliştiricilerden birine göre, yazılım sesin yapısını anlayabilmek için 20 dakikalık bir kayıt gerektiriyor ve ardından kaydı çoğaltabiliyor ve değiştirebiliyor. ⁵⁷ Şirketin teknolojiyi ne zaman yayınlayacağına dair bir zaman tahmini olmamasına rağmen, yazılım sesi değiştirme kabiliyetini gösterdi ve sahadaki gazeteciler bu kabiliyetin sadece gelişmesini bekliyorlar.

Lyrebird firması da benzer yetenekler geliştiriyor. Lyrebird'ün yazılımı, saatlerce konuşulan sesi dinleyerek herhangi bir sesteki karakterlerin, fonemlerin ve kelimelerin telaffuzlarını öğrenmek için yapay sinir ağlarını kullanır. Oradan tamamen yeni cümleler oluşturabilir ve hatta farklı tonlamalar ve duygular ekleyebilir.” ⁵⁸ Ancak Adobe'nin VoCo'su 20 dakikalık ses gerektirirken, Lyrebird'ün sistemi, konuşma oluşturmaya öğrendikten sonra yalnızca bir dakikalık örneklerle dayalı olarak herhangi bir sese uyum sağlayabilir. ⁵⁹ Zaman tahminlerine göre Lyrebird, yazılımı herkesin kullanımına sunmayı planladığı için teknolojisinin birkaç yıl içinde yaygınlaşacağını belirtiyor. ⁶⁰

Bazı durumlarda, zaman tahmini daha da kısa olabilir. İsrail merkezli bir ses kopyalama firması olan VivoText, kullanıcıların "bireysel kelimelerin ve cümlelerin üretildiği vurguyu, hızı ve mutluluk veya üzüntü seviyesini seçmelerine" ve ayrıca herhangi bir sesi ve kullanımı klonlamasına izin veren uygulamalar geliştirdi. kullanıcının istediği her şeyi söylemek için. ⁶¹ Bu çaba, bilgisayar tarafından üretilen mevcut sesin eleştirel olarak eksik olduğu sesin duygusal bileşenini yakalama yeteneğini geliştirecektir. Google,

⁵⁶ “Deneyisel Olalım: Adobe MAX Sneaks'in Arkasında,” *Adobe Blog* , 4 Kasım 2016.

⁵⁷ Adobe Inc., “#VoCo. Adobe MAX 2016 (Gizli Bakışlar),” 4 Kasım 2016.

⁵⁸ Bahar Gholipour, “New AI Tech Can Mimic Any Voice,” *Scientific American* , 2 Mayıs 2017.

⁵⁹ Gholipour, 2017.

⁶⁰ Lyrebird, “Büyük İnovasyonla Büyük Sorumluluk Gelir”, tarihsiz.

⁶¹ *The Economist* , 20 Nisan 2017 “İnsanların Konuşma Kalıplarını Tam Olarak Taklit Etmek Sorun Getirebilir”. Gelişmekte olan ürünleri hakkında daha fazla ayrıntı için VivoText'in web sitesine bakın.

diğer büyük teknoloji şirketleri arasında, son testlere göre insan konuşmasına oldukça benzer olarak derecelendirilen ses hizmetinin kalitesini artırmak için bir yazılım üzerinde çalışıyor. ⁶²

Lyrebird de dahil olmak üzere şirketler, yazılımlarının amacının kişisel AI asistanları ve engelli insanlar için konuşma sentezi gibi hizmetler için kullanılmak olduğunu belirttiler, ancak yazılımlarının potansiyel olarak olumsuz uygulamaları olabileceğini kabul ettiler. ⁶³ Kamuoyunun bilgiye olan güveninin risk altında olduğu bir zamanda, ses kayıtları gibi doğal güvenilirliğini koruyan kaynakların güvenilmez hale gelme potansiyelinin önemli etkileri olabilir. Örneğin, çok sayıda önde gelen siyasi şahsiyet için ses kayıtlarının mevcudiyeti göz önüne alındığında, bu ilerlemeler, bir liderin ağzına kelimeler koymayı bir bilgisayar kayıtlarını beslemek ve ardından yazılıma o kişinin ne söylemesi gerektiğini söylemek kadar kolay hale getirebilir. Bilgisayar tarafından oluşturulan bu ses dosyaları ne kadar inandırıcı olacak? Center for a New American Security'de yardımcı bir görevli olan Gregory Allen ile 2017 yılında yapılan bir röportaja göre, bir ila iki yıl içinde teknoloji, bilgisayar tarafından üretilen sesin eğitimsiz kulağı kandırabilmesini sağlayacak ve beş ila on yıl içinde teknoloji, ses sahteciliğinin "belirli adli analiz türlerinden kaçınmasını" sağlayacak. ⁶⁴

Adobe, diğerlerinin yanı sıra, adli tıp ve doğrulama sürecinin ne kadar süreceği belirsiz olsa da, ses manipülasyonlarını belirlemeye yardımcı olmak için filigran gibi dijital çözümler geliştirmeye ilgi duyduğunu belirtti. Genel olarak, bu teknolojilerin ilerlemesi, gerçeğin belgelenmesini destekleyen teknolojiden fabrikasyonun lehine olan dengeyi değiştirebilir ve yanlış bir ses klibiyle karşılaşma riskini yeni gerçeklik haline getirebilir. ⁶⁵

⁶² Aaron van den Oord, Tom Walters ve Trevor Strohman, "WaveNet Launches in the Google Assistant," *DeepMind Blog*, 4 Ekim 2017.

⁶³ Gholipour, 2017.

⁶⁴ Rob Price, "AI ve CGI, Bilgi Savaşını Dönüştürecek, Sahtekarlıkları ve İntikam Aldatmasını Arttıracak", *Business Insider*, 12 Ağustos 2017.

⁶⁵ Gholipour, 2017.

Uydurma Video: "Derin Sahtekarlıklar"ın Yükselişi

Resim oluşturma veya düzenleme, teknolojinin birkaç yıldır sahip olduğu bir özelliktir. Örneğin sosyal içerik web sitesi Reddit, hangi kullanıcıların görüntü işleme yazılımını kullanarak en iyi resmi oluşturabileceğini görmek için dostane yarışmalara ev sahipliği yapıyor. Bununla birlikte, yüksek kaliteli gerçekçi fotoğraflar veya videolar oluşturma yeteneği daha zorlu bir engel olmuştur. Son zamanlarda, bu zorluğun üstesinden gelmede önemli bir rol oynayan yazılım araçları tanıtıldı. ⁶⁶ Bu tür araçlardan biri, rekabetçi bir işlevi yazılıma entegre ederek çalışan ve bir ağ bir görüntü veya video gibi bir öge oluşturmaya çalışırken, diğer ağ ögeyi değerlendirip karar vermeye çalıştığı üretken çekişmeli ağlar (GAN'lar) olarak bilinir. gerçek görünüyor. ⁶⁷ İlk ağ, rakip ağı kandırmak için uyum sağlamaya devam ederken, yazılım daha gerçekçi görüntülerin veya videoların nasıl daha iyi oluşturulacağını öğrenir. ⁶⁸ Bu tür makine öğrenimi araçlarıyla Allen, "Yakın gelecekte amatörlerin bile foto-gerçekçi HD [yüksek tanımlı] video, ses ve belge sahtekarlıkları oluşturmaları mümkün olacak" diyor. ⁶⁹

Görüntüler söz konusu olduğunda, diğer araçlarla birlikte GAN'lar, gerçekçi görüntüler oluşturma yalnızca mümkün olmadığını, aynı zamanda önümüzdeki birkaç yıl içinde önemli ölçüde gelişeceğini göstermiştir. Örneğin, Google'daki bir makine öğrenimi sanatçısı, "önceden elde edilenlerin iki katından daha büyük, bir kenarı 768 piksel çözünürlüğe sahip hayali yüzlerin görüntülerini oluşturabildi". ⁷⁰ Ekim 2017'de bir

⁶⁶ Lee Ferran, "Beware the Crisis of 'Deep Fake News'" *RealClearLife* , 27 Temmuz 2018. Ayrıca bkz. Heritage Foundation'daki tartışma, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," panel tartışması, Washington, DC, 19 Temmuz 2018.

⁶⁷ "Sahte Haber: Henüz Hiçbir Şey Görmediniz," 2017. Ayrıca bkz. Ferran, 2018.

⁶⁸ Faizan Shaikh, "Üretici Düşman Ağlarına (GAN'lar) ve Vaatlerine Giriş Kılavuzu!" *Analitik Vidhya* , 15 Haziran 2017.

⁶⁹ Greg Allen ve Taniel Chan, *Yapay Zeka ve Ulusal Güvenlik* , Cambridge, Mass.: Belfer Bilim ve Uluslararası İlişkiler Merkezi, Harvard Kennedy Okulu, Temmuz 2017, s. 29. Ayrıca bkz. Will Knight, "Bu İnanılmaz Gerçekçi Sahte Yüzler, Algoritmaların Artık Bize Nasıl Bulaşabileceğini Gösteriyor," *MIT Technology Review* , 14 Aralık 2018e.

⁷⁰ "Sahte Haber: Henüz Hiçbir Şey Görmediniz," 2017.

NVIDIA adlı grafik işleme birimi şirketi, bir görüntü örnekleri veritabanında yazılımı eğitmek için GAN'ları kullanarak insanların ve nesnelerin HD görüntülerini oluşturma yeteneğini gösterdi. ⁷¹ Oluşturulan görüntülerin bazıları bozuk olmasına rağmen, şirket, araçlar, odalar ve tüm binalar gibi insanların ve öğelerin yüksek kaliteli görüntülerini oluşturabildi ve bu, araştırma ekibinin son derece gerçekçi fotoğraflar üretmenin erişilebilir olduğuna inanmasına yol açtı. ⁷²

Araştırmacılar ayrıca son zamanlarda metin açıklamalarını görüntülere dönüştürerek küçük ama fotogerçekçi görüntüler geliştirebildiler. Yazılım, “Küçük kuşun baştan kuyruğa kırmızıdan griye giden tüyleri olan kırmızı bir kafası var” ve “Etrafta duran ve poz veren bir grup insan gibi cümle açıklamalarına dayalı çeşitli görüntüler üretebiliyor. bir resim için.” ⁷³ Gelecekteki gelişmeler, tam HD görüntüler oluşturmak için çözünürlüğü ve boyutu iyileştirmeye çalışacak ve Wyoming Üniversitesi'nde sinir ağlarını kullanarak görüntü üretme konusunda çalışan bilgisayar bilimi yardımcı doçenti Jeff Clune'a göre, “muhtemelen sipariş üzerine. yılların değil, yılların.” ⁷⁴

Bilgisayar tarafından oluşturulan görüntüler oluşturma yeteneği video prodüksiyonundan daha ileri düzeyde olsa da, yakın zamanda gerçekçi videolar oluşturma mümkün olabileceğini gösteren birkaç yeni gelişme olmuştur. Bu gelişmelere bir örnek, ortak bir web kamerası ile birlikte bir kullanıcının herhangi bir kişinin yüz hareketini değiştirmesine izin verebilen ABD'li ve Alman araştırmacılar tarafından üretilen yazılımdır.

⁷¹ Tero Karras, Timo Aila, Samuli Laine ve Jaakko Lehtinen, “Geliştirilmiş Kalite, Kararlılık ve Varyasyon için GAN'ların Aşamalı Büyümesi,” *Altıncı Uluslararası Konferans Öğrenme Temsilleri, Konferans Bildirileri*, Vancouver, Kanada, 2018; Hillary Grigo-nis, “AI, İnsanların Bilgisayar Tarafından Oluşturulan En Gerçekçi Görüntülerinden Bazılarını Oluşturuyor,” *Digital Trends*, 30 Ekim 2017.

⁷² Karras ve diğerleri, 2018.

⁷³ Han Zhang, Tao Xu, Hongsheng Li, Shaoting Zhang, Xiaogang Wang, Xiaolei Huang ve Dimitris Metaxas, “StackGAN: Metinden Foto-Gerçekçi Görüntü Sentezine, Yığılmış Üretken Düşman Ağlar”, *IEEE Uluslararası Bilgisayarla Görme Konferansı*, Konferans Bildirileri, Venedik, İtalya: Elektrik ve Elektronik Mühendisleri Enstitüsü, Ekim 2017, s. 8–14.

⁷⁴ James Vincent, “Yapay Zeka, Sahte Görüntüler ve Videolar Yapmayı Hiç Olmadığı Kadar Kolaylaştıracak,” *The Verge*, 20 Aralık 2016.

gerçek zamanlı olarak kaydedilmiş bir videoda. ⁷⁵ Bu yazılımı kullanarak, göze çarpan bir figürün yüz ifadelerinin kaydı, gerçek zamanlı olarak kullanıcının yüz ifadeleriyle eşleşecek şekilde değiştirilebilir ve bu, göze çarpan figürün kullanıcının istediği her şeyi söylüyormuş gibi görüldüğü yeni bir video üretilir. ⁷⁶

Başka bir örnek, Washington Üniversitesi'ndeki araştırmacılar tarafından geliştirilen ve bir hoparlörde eşleşen ağız şekilleri oluşturmak için yazılım eğiterek ses kliplerini gerçekçi videoya dönüştürmeyi amaçlayan yazılımdır. ⁷⁷ Yazılım şu anda bir seferde bir kişinin konuşma kalıplarını öğrenmek için tasarlanmıştır, ancak ekip, yazılımın konuşma kalıplarını tanıma kapasitesini genişletmesine yardımcı olmak ve bunu daha az veri ile yapmak da dahil olmak üzere gelecekteki gelişmeleri belirledi. ⁷⁸ Ayrıca, “yüzme havuzunda yüzmek” veya “golf oynamak” gibi metin komutlarından videolar oluşturmak için teknolojik gelişmeler olmuştur. ⁷⁹ Şimdilik, oluşturulan bir videonun üretebileceği süre, çözünürlük ve hareketle ilgili yetenek sınırlıdır, ancak gelecekteki adımlar, oluşturulan videolarda insan etkinliğinin kalitesini iyileştirmek için insan pozu ve iskelet özellikleri oluşturmayı içerir. ⁸⁰ Bu yeteneğe ulaşma potansiyeli, bu iki adımın nasıl ele alınacağına ilişkin bazı ön araştırmalar halihazırda mevcut olduğundan, önümüzdeki on ila 15 yıl içinde kesinlikle mümkündür. ⁸¹

⁷⁵ Adario Strange, “Yüz İzleme Yazılımı, Herkesin Gerçek Zamanlı Olarak Her Şeyi Söylemesini Sağlıyor,” *Mashable*, 20 Mart 2016.

⁷⁶ Jutus Thies, Michael Zollhöfer, Marc Stamminger, Christian Theobalt ve Matthias Nießner, “Face2Face: Real-Time Face Capture and Reenactment of RGB Videos,” *IEEE Bilgisayarla Görme ve Örüntü Tanıma Konferansı*, *Konferans Bildirileri*, Las Vegas, Nev.: Elektrik ve Elektronik Mühendisleri Enstitüsü, 2016.

⁷⁷ Jennifer Langston, “Lip-Syncing Obama: New Tools Turn Audio Clips to Realistic Video,” *UW News*, 11 Temmuz 2017.

⁷⁸ Langston, 2017.

⁷⁹ Yitong Li, Martin Renqiang Min, Dinghan Shen, David Carlson ve Lawrence Carin, “Metinden Video Üretimi,” *Otuz İkinci AAAI Yapay Zeka Konferansı*, *Konferans Bildirileri*, New Orleans, La.: Yapay Gelişimi Geliştirme Derneği Intelligence, Şubat 2018, s. 3–6.

⁸⁰ Li ve diğerleri, 2018, s. 5–8.

⁸¹ Haoye Cai, Chunyan Bai, Yu-Wing Tai ve Chi-Keung Tang, “Deep Video Generation, Prediction and Completion of Human Action Sequences,” *Avrupa Bilgisayar Konferansı Vision 2018, Conference Proceedings*, Münih, Almanya, Eylül 2018, s. 8.

Gerçekçi görüntüler veya videolar oluşturma yeteneğinin nasıl tehlikeli sonuçlar doğurabileceğini hayal etmek zor değil. Teknoloji bu prodüksiyonun kalitesini iyileştirdikçe, özellikle ses yazılımındaki gelişmelerle birleştiğinde, gerçek olayları üzerinde oynanmış veya yapay olanlardan ayırt etmek muhtemelen daha zor hale gelecektir. Sonuç, belirli bir kişinin istediği her şeyi söyleyen ve yapan, bilgiye olan toplumsal güveni aşındıran önde gelen isimlerin görüntüleri olabilir. ⁸² GAN'ları tanıtan araştırmacı bilim adamı Ian Goodfellow, 2020 yılına kadar çok inandırıcı YouTube sahteleri oluşturma'nın mümkün olabileceğini iddia ediyor. ⁸³ Bu gelişmeler, bilgi yaratmanın yanı sıra ses, görüntü veya gerçek olayların videolarının oluşturulabileceği bir atmosfer yaratabilir. sahte olduğu iddia edildi. Savunma İleri Araştırma Projeleri Ajansı'nın (DARPA) medya adli tıp çalışmalarının proje yöneticisi Matt Turek, "Birkaç yıl içinde göreceğimizi düşündüğüm şey, gerçekleşmemiş olayların sentezidir. Farklı perspektiflerden çekilmiş birden fazla görüntü ve video, farklı kameralardan gelmiş gibi görünecek şekilde oluşturulacak." ⁸⁴

Üstelik çıta tamamen gerçekçi ve doğru görüntüler kadar yüksek olmayabilir. Çoğu çevrimiçi video ve resim, bazen dosya boyutlarını sıkıştırma ihtiyacının bir sonucu olarak zaten bulanık veya bozuk. Bu sistemlerin performansının, pek çok izleyiciyi ürünlerinin orijinalliğine ikna etmek için kristal berraklığında senteze yükseltilmesi gerekemeyebilir.

Zamanla, oldukça gerçekçi hareketli görüntüler oluşturma potansiyeline sahip bilgisayar tarafından oluşturulan görüntüler (CGI) ve benzer teknolojiler, tüketici pazarlarına girerek, özel şirketler ve bireyler tarafından hiper gerçekçi bilgisayar tarafından oluşturulan görüntüleme ve video prodüksiyonunun yaygın şekilde kullanılmasına olanak tanıyacaktır. Gelişmiş AI yeteneklerine sahip botlar, sosyal medya platformunda insanlara (fiziksel ve görsel olarak) benzeyecek.

⁸² Vincent, 2016.—

⁸³ "Sahte Haber: Henüz Hiçbir Şey Görmediniz," 2017.

⁸⁴ Joshua Rothman, "Afterimage," *New Yorker*, 12 Kasım 2018, s. 40.

formlar ve VR ve AR uzayları, gerçekleri CGI varlıklarından ayırt edemeyeceğimiz kadar iyi.⁸⁵

Gözetim sistemleri

Bulut veya IoT ile bağlantılı hemen hemen her yeni teknoloji, 2030 ile 2035 arasında bir zamana kadar bir tür gözetim veya "sousveillance" amacına hizmet *edebilecektir*. insanların internet alışkanlıkları hakkında veri toplama, cep telefonu konumları aracılığıyla hareketlerini kaydetme, ev tabanlı sesle etkinleştirilen asistanlar tarafından ses kaydı ve daha fazlası.) Bir kişinin veya grubun faaliyetinin görünürlüğü ve gözetimi, mutlaka hareketlerini, iletişimlerini, işlemler ve davranışlar. Gerçekten de, ortaya çıkan şey bir tür *ortamdır*. büyük veri hazinelerinin toplandığı *gözetim sistemi* ve hükümetler ve diğer aktörler için teorik olarak yararlı veya ticari amaçlar için tasarlanmış, ancak yine de bir nesil önce en otoriter hükümet için bile düşünülemez olan bireyler hakkında bir dereceye kadar veri toplamayı yansıtan şekillerde işlenmiş ve teorik olarak erişilebilir. Aynı zamanda, yapay zekanın ilerlemesi, bu sistemleri eğitmek için gerekli yakıtı sağlamak için sürekli artan veri toplama talebi yaratıyor ve Amerikalılar hakkında devasa bilgi yığınlarını süpürmek için ek finansal teşvikler üretiyor.

2030 yılına kadar, hareket büyütme ve mikroskop yazılımı (Eulerian Video Magnification [EVM] olarak adlandırılır) gözetim ve akıllı telefon kameralarında ve video kayıtlarında standart olacak; bu araçlar, aksi takdirde görünmez olabilecek ayrıntıları ortaya çıkarır (örneğin, göz kaslarındaki küçük hareketler, kan akışı, görünüşte sabit nesnelerdeki mikroskobik hareketler). Ayrıca dünyada çoğu insan taşıyabilecek en az 1 milyar insansız hava aracı olacak.

85—Jesus Diaz, "CGI'nın Garip, Vahşi Geleceği," *Fast Company*, 19 Ekim 2017.

gözetim ekipmanı ve veri alma ve iletme yeteneğine sahiptir. ⁸⁶

Çoğu nanoteknoloji, ileri yaşam bilimlerinden (örneğin, cerrahi hassas aletler ve hücresel düzeyde teknoloji) gelecektir. Hassas yeteneklere ve HD görüntüleme ve videoya sahip daha küçük cihazlar yaratma çabası, gelecekteki gözetim donanımlarında benzer çabalara yardımcı olacaktır. Günümüzün en küçük gözetleme insansız hava araçları, kabaca küçük bir böcek boyutundadır ve hala erken geliştirme aşamasındadır. ⁸⁷

Sousveillance'ın rolü hızla büyüyor. Google ve Facebook tarafından bireyler hakkında toplanan bilgilerle ilgili son tartışmalar, gizli gözetleme sorununa ilişkin çok daha geniş bir tartışmanın yalnızca başlangıcıdır. On ila 15 yıl içinde, dünya nüfusunun yüzde 90'ı bir internet varlığına sahip olacak; Yüzde 80'i ücretsiz ve sınırsız veriye sahip olacak; evlere yönelik internet hizmetlerinin yüzde 50'den fazlası IoT'ye bağlı ev aletleri ve ev cihazları aracılığıyla olacak; 1 trilyon cihaz IoT'ye bağlanacak; ve gözetim, cihazlara ve ağlara erişimin yanı sıra büyük veri yönetimi, madencilik ve analiz meselesi olacaktır. ⁸⁸ Sağlık ve duygusal durumları değerlendiren giyilebilir cihazlar ve implantlar, insanların ruh hallerini ve bakış açılarını bildirmede dikkate değer derecede bir doğruluk sağlayacaktır. ⁸⁹

Halihazırda, bilgisayar korsanlarının ve saldırganların yükselen ortam gözetim sisteminden çalınan verileri nasıl kullanabileceğine dair endişeler artıyor. Office of Personel Yönetimi kayıtlarının çalınması, Cambridge Analytica'nın Facebook üzerinden arkadaş ve iletişim verileri edinmesi ve diğer veri tabanı hırsızlığı ve bilgisayar korsanlığı vakalarında, devletler ve kuruluşlar bu tür verilere erişimi zorlayıcı amaçlar veya rekabet avantajı için kullanmıştır. Etkili sosyal manipülasyona giden bu potansiyel yol, yalnızca ortam gözetimi süreci derinleştikçe büyüyecektir.

86 Hao-Yu Wu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand ve William Freeman, "Eulerian Video Magnification for Revealing Subtle Changes in the World", *ACM Transactions on Graphics*, Cilt. 31, Sayı 4, 2012.

87 Gareth Evans, "Robotik Böcekler, 'Duvarda Uçan' Gözetleme Mızrağı'na Yepyeni Bir Anlam Katıyor," *Army Technology*, 16 Mart 2015.

88 Yazılımın ve Toplumun Geleceği Küresel Gündem Konseyi, 2015, s. 7.

89 Tiku, 2018, s. 55.

Örnek teknikler arasında, “doxfare”in yeni versiyonları (kişisel veya gizli bilgiler içeren belgeleri çalmak ve bunları şantaj amacıyla kullanmak ve başka bir devletin siyasi sürecine müdahale etmenin diğer yolları),⁹⁰ ve doğrudan siyasi yöntemler gibi halihazırda iyi kurulmuş birkaç teknik yer almaktadır. Giderek daha güçlü çıkarımsal tercih modelleri aracılığıyla manipülasyon - ama aynı zamanda sosyal bozulma ve güvenin bozulması stratejilerini güçlendirmek için konum, ruh hali, davranış, arkadaşlar, bağlantılar ve daha pek çok konuda toplanan verileri kullanan yeni yaklaşımlar.

Sonuç: Hızla Değişen Bir Bilgi Dünyası

Bu karmaşık ve birçok yönden birbirine bağlı teknolojiler grubu, gelişmiş ekonomilerde bilgi dünyasının dönüşümünü hızlandırma potansiyeline sahiptir. Bu teknolojilerin yayılımı veya yeteneklerindeki mevcut eğilimleri yansıtmak veya etkilerinin doğrusal olacağını varsaymak çok basit olacaktır. Örneğin, video sahtekarlığının, hiç kimsenin gördüğü herhangi bir şeyin gerçek olup olmadığına dair net bir fikre sahip olmadığı bir gelecek yaratması gerekmez; Nesnelerin İnterneti, yeni güvenlik açıkları kadar veya daha fazlası kadar ağ bağlantılı bir tür esneklik sağlayabilir; ve hükümetler - hatta otokratik olanlar bile - gözetim sistemlerinin kullanımını sınırlamaya zorlanabilir. Bu teknolojilerin sürekli ortaya çıkmasından kaynaklanan en kötü durum, distopik sonuçları varsaymak, en iyimser sonuçları varsaymak kadar yanlış olacaktır.

Bununla birlikte, bu kısa inceleme, dış aktörlerin bu teknolojileri ve sistemleri manipüle etme, bozma ve kontrol etme potansiyelinden ileri toplumların istikrarı ve tutarlılığına yönelik önemli ve tartışmalı olarak artan riskleri açıkça ortaya koymaktadır. Bu teknolojiler aynı zamanda, kasıtlı manipülasyon olmasa bile, sosyal kaynaşmaya ve demokratik yönetişime zarar verecek şekilde bilgikürenin karakterini değiştirmek için yerleşik bir potansiyel içerir: ortak bir gerçekliğin düşüşünü hızlandırmak, kurumsal egemenlik sistemlerini güçlendirmek

90 Ido Kilovaty, "Doxfare: Politik Olarak Motive Edilen Sızıntılar ve Silahlaştırılmış Bilgi Çağında Müdahale Dışı Normunun Geleceği," *Harvard National Security Journal*, Cilt. 9, No. 1, 2018.

bireyler üzerinde ve ortalama vatandaşlar tarafında yabancılaşma duygusunu şiddetlendiriyor. Belki de bu incelemeden çıkarılması gereken baskın ders, Amerika Birleşik Devletleri ve diğer birçok ulusun bir geçiş anıyla karşı karşıya olduğudur. Bu teknolojilerin kolektif etkisi dönüşümsel olabilir ve toplumlar ve hükümetler, etkilerini şekillendirme çabalarında giderek daha bilinçli ve yönlendirici olma gerekliliğiyle karşı karşıya kalabilirler.

Aşağıdaki üç bölüm, bu teknolojilerin evrimi ve düşmanca sosyal manipölasyon için sundukları potansiyel için üç potansiyel senaryo sunarak bu gereksinim için bir bağlam sağlar. Her senaryo, hayal ettiği trendlere yol açan fırsatları ve umutları tanımlar, ancak her biri kuşkusuz riskleri öne çıkarmak için tasarlanmıştır. Tahminler olarak sunulmazlar; vurgu, özellikle bu ilerlemelerin birleşik etkisinin tehlikeler oluşturabileceği yollar üzerindedir ve gerçek sonuçların bir şekilde farklı bir etki yelpazesini yansıtması muhtemeldir. Bununla birlikte, ortaya çıkan teknolojilerin karakteri göz önüne alındığında, bu senaryoların her biri tamamen akla yatkındır.

Gelecek 1: Gerçekliğin Ölümü (2025 Senaryosu)

Metodoloji Hakkında Bir Not

Düşmanca sosyal manipölasyonun nasıl ortaya çıkabileceğine dair olası senaryoları araştırmak için son üç bölümde incelenen eğilimlere ve verilere güvendik: bilgikürenin gelişen manzarası üzerine araştırma; tutumlar, tutum değışikliği, ikna ve sosyal güven üzerine sosyal bilim bulguları; ve belirli teknolojilerin gelişen karakteri. Bu senaryolar, bilgi küresi olarak adlandırdığımız toplumda bilginin rolü için üç olası geleceğı göstermek üzere tasarlanmıştır. Her durumda, bilgiye dayalı saldırganlığın demokrasiye saldırmak için her senaryonun unsurlarını nasıl kullanabileceğini açıklıyoruz. 1

Bu anlatıları "gelecek" olarak adlandırıyoruz, çünkü bunlar belirli, olaya dayalı senaryolardan ziyade ortaya çıkabilecek bir dünyanın genel tanımlarıdır. Beş, Altı ve Yedinci Bölümlerin her biri, bu geleceklerden birini, geleceğın bir ilk özeti, o geleceğın belirli unsurları hakkında bir veya daha fazla bölüm ve o çevredeki sosyal manipölasyon risklerini açıklayan bir sonuç bölümü aracılığıyla açıklar. Her bölüm geleceğı katkıda bulunan teknolojik, sosyal ve politik faktörlerin bazı tartışmalarını içerir. Gelecekler dramatize edilir ve birçok icat edilmiş potansiyel gelecekteki gelişmeyi içerir, ancak olaylar mevcut eğilimler üzerine araştırmalara sıkı sıkıya bağlıdır. Onların amacı

1 Birden fazla otokratik rejimin bu teknolojileri yerel ve uluslararası etki için kullanma yollarının bir açıklaması için bkz. Juan Pablo Cardenal, Jacek Kucharc-zyk, Grigorij Mesežnikov ve Gabriela Pleschová, *Sharp Power: Rising Authoritarian Influence*, Washington, DC: National Endowment for Democracy, Aralık 2017.

ileri demokrasilerin bilgi ortamlarının gelişen geleceği hakkında bir dizi görüntüyü anlatısal yollarla hayata geçirmenin bir parçası.

Bu gelecekler tahmin değil. Bunları ana hatlarıyla belirtirken, bu geleceklerden herhangi birine yansıyan belirli faktör kombinasyonunun açıklandığı gibi ortaya çıkmasının muhtemel olduğunu öne sürmüyoruz. Açıklayıcı ve düşündürücüdürler, düşmanca sosyal manipülasyonun ve sanal toplumsal savaşın gelecekteki potansiyel yörüngesi hakkında tartışmayı kışkırtmak için tasarlanmıştır. Ancak her biri, değişen bilgi küresi, etki ve güvenin sosyal bilimi ve gelişen teknolojilerin karakteri üzerine derinlemesine araştırmalara dayanıyor. Senaryolar, gelişmekte olan teknolojilerin doğasında bulunan üç olası tehlikeyi göstermek için tasarlanmıştır. Bu sonuçların bazılarını yumuşatması muhtemel olan, sosyal medya platformlarının uydurma bilgilere karşı koyma çabaları gibi, henüz tamamlanmamışsa da artan çabalar gibi, devam etmekte olan bazı zıt eğilimler var. Ancak, gelişmekte olan teknolojiler ve birçok ülkedeki hükümetler ve kurumlar , gelişen bilgi dünyasının karakterini şekillendirmek için aktif olarak çalışmazlarsa, aşağıda açıklanan senaryolar makul olmaya devam ediyor .

Ayrıca, bu üç gelecek birbirini dışlayan olası sonuçlar olarak sunulmamaktadır. Her biri, bilgi dünyasındaki eğilimlerden alınan tek bir öncü değişken etrafında inşa edilmiştir: Biri, gerçek gerçekler ve olaylar ile uydurma veya yanlış olanlar arasındaki ayrımın herhangi bir katı ve nesnel anlayışının düşüşüne odaklanır; biri yankı odalarının yükselişine ve kendi kendini güçlendiren inanç ve bilgi silolarının parçalanmış bir bilgi gerçekliğine çöküşüne odaklanır; ve biri algoritmik karar vermenin artan rolüne odaklanır. Herhangi bir gerçek gelecek, bu ana itici güçlerin bir dereceye kadar içermesi muhtemeldir ve bir dereceye kadar örtüşürler; bilgi siloları dünyası aynı zamanda nesnel gerçeklik duygusunun solduğu bir dünyadır. Sırasıyla her birine odaklanarak, gelecekler ortaya çıkan bir bilgi dünyasının çeşitli yönlerini ayrıntılı olarak araştırmamıza izin veriyor.

Son olarak, bu geleceklerin 2023 ve 2028 yılları arasında gelebileceğini öne sürdük. Seçilen tarihler biraz keyfi olsa da, bu tarihler, teknoloji ve yapı açısından bilgi küresinin bunlara ne kadar yakın görüldüğüne göre atanmış olsalar da. gelecekler. Ancak tarihler tahmin anlamına gelmez.

Genel Gelecek

“Gerçeklik” 2023'te öldü.

Böyle kademeli ve belirsiz bir süreçte belirli bir tarih eklemek belki de cüretkardır. Yine de o yıl, görünüşte uzun ve olaylı iki yıl önce yaşanan birçok gelişme, bunun insan yaşamında yeni bir hakikat-sonrası, gerçek-sonrası, gerçeklik-sonrası çağın eşiği olarak görüleceğini gösteriyor. Objektif, tekil, tanımlanabilir bir gerçeklik kavramı, toplumun birçok köşesinde şimdiden alay konusu ediliyor ve büyüleyici bir anakronizm olarak anılıyor.

Bu cesur iddiayı haklı çıkarmak için 2023'te tam olarak ne oldu? Her biri on yıldan fazla bir süredir olgunlaşmakta olan eğilimlerin özünü yansıtan birkaç şey. Bu gelişmelerin ilki ve en kapsamlısı, şimdi bildiğimiz şekliyle bilgi ortamının temel özelliğini oluşturuyordu: Basitçe söylemek gerekirse, elle tutulur görünen gerçekliği sıfırdan üretme yeteneği artık olağan hale geldi.

Bazı açılardan, bu, on yıllardır beklenen, olayların anlamının ve öneminin evrensel olmadığı ve üzerinde anlaşmaya varıldığı, ancak olumsal ve tartışıldığı bir “postmodern” gerçekliğe yönelik ampirik eğilimlerin doğal sonucudur. Bu eğilimin kökleri, dar ve geleneksel düşünme biçimlerini yıkmak ve bireylere eşî görülmemiş bir ifade fırsatı sağlamak için bazı yaratıcı ve umutlu çabalarda yatıyordu. Bu eğilimlerin temel güdüsü ve etkisinin çoğu – olaylara öznel bir bakış açısı edinme hakkı – hatırlanmalıdır, güçlendirici olmuştur. İster hükümetlerden isterse toplumsal mutabakattan olsun, bireyin kısıtlamalara ve baskıya karşı güçlendirilmesine yönelik daha geniş yörüngeyle yakından iç içe geçmiş şekillerde ortaya çıkmıştır. Birkaç modern sanatsal ifade okulu, düşünce ve belirli davranış biçimleri üzerindeki toplumsal kısıtlamaların kademeli olarak bozulması ve gerçekliği karıştıran eğlence biçimleri de dahil olmak üzere, şimdi gerçekliği büken (veya gerçekliği yok eden) ifadeler olarak tanımlananların çoğu, evrensele karşı bireysel bakış açısının bu daha temel ifadesinden doğmuştur.

Ancak postmodern fikirlerin eleştirmenlerinin uzun süredir uyardığı gibi, bu özneleşme ivmesini yavaşlatmanın zor olduğu kanıtlanmıştır.

insan algısı. Hiçbir baskın anlatı ya da geleneksel bilgelik doğru ya da geçerli olmadığında, bazılarına göre, *herhangi bir* genelleştirilmiş gerçek iddiasının böyle bir statüye nasıl talip olabileceği artık açıktır . Bireylerin olaylar hakkında benzersiz bir ses çıkarmasını sağlayan teknolojiler ve bakış açıları, kısa sürede bu açılımı milyonlarca kişiye sundu. Gerçeklik, paylaşıldığı kadar kişiselleştirildi; bu, olayları yorumlama kendi haklarını talep etmeye çalışan işletmeler de dahil olmak üzere toplumdaki bazı büyük kurumlar tarafından hızlandırılan bir eğilim.

Uzun vadeli bir perspektiften bakıldığında, aslında genel eğilim yeni bir şey değildi, çünkü kelimesi kelimesine gerçeğin yerine metaforik olanın ikame edilmesinin uzun bir geçmişi vardır. 20. yüzyıl boyunca, resmin gerçekliği, doğrudan temsilden ziyade soyutlamaya ve yaşamın dışavurumcu yorumuna yol açtı. Kurgu dışı yazı ve gazetecilik, gerçeklerin doğruluğunu genişleten yeni biçimleri somutlaştırdı. Doğrulanabilir, otantik bir anı kavramı, en azından bir süre için, meşru olarak kabul edilen sahteciliklere yol açtı; “biyopiklerde” tarihsel doğruluğa bağlılık, yerini sanatsal lisansa bıraktı. En popüler televizyon programlarının çoğu, dramayı sahnede yönetilen gerçeğe yakınlık iddialarından inşa etti - yani, anlatı odaklı icatlardan inşa edilen “gerçeklik” şovları.

Bu en temel eğilimin kökleri, gerçekleri ve gerçekliği manipüle etmek için onlarca yıllık kurumsal çabalara dayanıyordu. Muhtemelen tüm bu çabaların kaynak kodu, tütün lobisinin sigaranın kansere yol açtığını öne süren bilimsel araştırmalara olan inancı yok etme çabalarıydı. Endüstri, geçmiş programların tüm ayırt edici özellikleriyle büyük bir çaba sarf etti: araştırmaların arkasındaki bilim adamlarının ve kurumların meşruiyetine saldırmak; çoğu ölümcül derecede taraflı olan, telafi edici araştırmalar üretmek için dost bilim adamlarını işe almak; kamuoyunu şekillendirmek için kitlesel halkla ilişkiler kampanyaları için ödeme yapmak; ve mesajını desteklemek için ünlü spor yıldızlarını ve televizyon kişiliklerini işe almak. 2 Amaç, sorunu çerçevelemek ve anlatıyı, nüfusun en azından önemli bir azınlığının sorunu nasıl anladığını kontrol ederek şekillendirmektir.

2 Bu kampanyaların kapsamlı bir değerlendirmesi için bkz. Ari Rabin-Havt, *Lies, Incorporated: The World of Post-Truth Politics* , New York: Anchor Books, 2016.

Bu anlamda, insan yaşamının çoğu, kelimenin tam anlamıyla "gerçek" olmaktan ziyade sanatsal, yaratılmış ve hayal edileni - bir zamanlar kültürel anlamdan çok daha ontolojik bir anlamda, yaşamın Hollywoodlaştırılmasını - yansıtmaya başlamıştır. hayal edildi. ³ ("[a]rt gerçek değildir; sanat, gerçeği tanımamızı sağlayan bir yalandır" diyen Picasso'ydu. ⁴ Eğlence sektöründeki birçok kişinin bu duyguyu ne kadar ciddiye alacağını hayal bile edemezdi.) Öykü 20. yüzyılın sonları ve 21. yüzyılın başlarında, gerçek ile sahte, gerçek ile gerçek dışı arasındaki azalan bariyerlerden biriydi. Birkaç güçlü teknoloji, bu harmanlamayı dramatik şekillerde hızlandırdı.

Ortaya çıkan bu kalıplar, kısmen rahatsız edici ama kaçınılmaz bir gerçek tarafından körüklendi: İnsanlar, gerçekler yerine rahatlığı ve hazzı tercih ediyor. Fried-rich Nietzsche, gerçekliği büken mevcut eğilimlerin ileri görüşlü bir tahmininde, "İnsan gerçeği ancak sınırlı bir ölçüde ister," diye savundu. "Gerçeğin hoş, yaşamı koruyan sonuçlarını arzular; sonuçsuz saf bilgiye kayıtsızdır, potansiyel olarak zararlı ve yıkıcı gerçeklere bile düşmandır." Nietzsche, insan bilincinin "bilgi için değil , şeylerin *kontrolünü ele geçirmek* için tasarlanmış bir soyutlama ve basitleştirme aygıtı" olduğuna inanıyordu. ⁵

Son birkaç on yılda şirketler, haber medyası ve eğlence endüstrisi, insan doğasının bu temel yönünü onunla savaşmak yerine kabul etmeye ve onun içinde çalışmaya giderek daha fazla karar verdi. İnsanlara istediklerini veriyorlar ve sosyal bozulma, yavaşlayan büyüme, artan eşitsizlik ve giderek nüfuz edilemez kurumlar karşısında yabancılaşma zamanında, istediklerinin çoğu zaman sansasyonel, aşırı olarak algılandığı görülüyor. ve izleyicinin sosyal üyelik duygusunu derinleştirmesine izin veren bir tür dış gruba karşı hedeflenmiştir.

³ Stacy Schiff, "İnteraktif Gerçek," *New York Times* , 15 Haziran 2005.

⁴ David Shields, *Reality Hunger: A Manifesto* , New York: Knopf, 2010, s. 14, 32, 34-35, 40-42.

⁵ Friedrich Nietzsche, *Hakikat ve Yalan Üzerine: Seçilmiş Yazılar* , çev. ve ed. Taylor Carman, New York: Harper Perennial, 2010, s. 24, 121.

Bu geleceğe önemli bir katkıda bulunan eğilim, gerçekliğe aracılık eden kurumların ve yetkililerin devam eden ve aslında hızlanan çöküşü olmuştur . Yeni yıla sadece birkaç gün kala 2023'teki ilk olay, Facebook'un *New York Times*'i satın aldığını duyurmasıydı . Genellikle bir hayırseverlik ve sosyal sorumluluk eylemi olarak görülüyordu; Bir dizi skandal, şüpheli popülist bilgisayar korsanlarından gelen tutarlı saldırılar ve ana şirketi ayakta tutan birkaç yayın dışı girişimin düşüşüyle sarsılan *Times* , 2021'de önemli yeni yatırımlar olmadan nihai iflasa yöneldiğini açıklamıştı. (Genel gazete geliri yaklaşık 2010'dan beri yılda yüzde 4'ten yüzde 5'e düşüyor. 6) Facebook, yasayı, platformlarındaki sahte veya taraflı bilgilerle mücadele etmek için 2017'de başlayan çabalarının bir devamı olarak faturalandırdı. Şirket ve kurucusu Mark Zuckerberg, Jeff Bezos'un *Washington Post*'u alırken yaptığı gibi, *araştırmacı gazeteciliğe bağlılıklarında çabucak ısrar etseler de, Times*'i tamamen dijitalleştirmek (veya sanallaştırmak) ve entegre etmek için bir dizi plan açıkladılar. Facebook'un kullanıcı odaklı arayüzüne. Zuckerberg gururla " Facebook Haber Kaynağınız artık - kelimenin tam anlamıyla - *New York Times* olacak" dedi. "Bir ve aynı olacaklar."

Sorun, elbette, Facebook'un sonuçta ortaya çıkan beslemeyi, insanların neyi okumak "isteyeceğine" karar veren aynı algoritma tarafından yönetilen model aracılığıyla önemli ölçüde filtrelemeyi planlamasıydı. İş modeli, insanlara neyi "bilmeleri" gerektiğini söylemeden, tıklamalara ve tercihlere dayanıyordu. Okuyucular, doğrudan göz atarak *Times*'in tamamına erişmeye devam edebilir, ancak çoğu zaman almaz. Sonuç, kolektif farkındalığın ulusal düzeyde paylaşılan birkaç kanalından birinin parçalanması oldu. Ulus için "kayıt defteri" olan *Times* , artık tamamen kullanıcı odaklı bir algoritmaya eklenmiş bir marka adından başka bir şey değildi. Muhabirler, bazıları "araştırmacı" raporlar olmak üzere hikayeler üreten haber odalarında çalışmaya devam edecekti. Ancak onları okuyanlar tercihlere bağlı olacaktır. Bu geliş-

6 Regina Joseph, "Geleceğe Bakış: Influence'ın Yeni Ustaları Tarafından Gizli Bir Devrim", Weston Aviles ve Sarah Canna, ed. , *Yükseliş Çağında Etki Üzerine Beyaz Kitap Connectedness* , Washington, DC: ABD Savunma Bakanlığı, Ağustos 2017, s. 11.

Bu açıklama, kamu medyasında temel olgu iddialarının bazı temellerini sağlayabilen güvenilir müdahil kurumların devam eden düşüşünde bir başka adımı temsil ediyordu.

Trend sadece medyadan çok daha fazla kurumu etkiledi. Yetkililere yönelik artan şüpheciliğin öne çıkan bir diğer hedefi de akademi. Amerika Birleşik Devletleri'ndeki muhafazakarlar uzun zamandır üniversiteleri liberalizmin kaleleri olarak görüyorlardı ve bu algı, geçtiğimiz birkaç yılda, kimlik politikasının konuşmayı kısıtlayan fikirlerini destekleyen, profesörleri sözde saldırgan ifadeler kullandıkları için işten çıkarma hakkı için savaştıkça yoğunlaştı. muhafazakarların tamamen makul bulduğu görüşler. Aynı zamanda, yüksek öğretimde sosyal bilimsel araştırmanın güvenilirliği, sosyal bilim araştırmalarındaki birçok yüksek profilli “bulgu”nun basitçe tekrarlanamayacağı gerçeği için bir terim olan kalıcı bir “kopyalama krizi” tarafından sorgulanmıştır. . Sonuç, herhangi bir yeni çalışma hakkında şüphe uyandırmak oldu. 2022-2023'e kadar anketler, Amerikalıların yalnızca yüzde 15 ile yüzde 20'sinin üniversitelerin "gerçeğin nesnel arayışı için yerler" olarak misyonlarını sürdürdüklerine "yüksek güven" duyduğunu gösteriyordu.

Bu eğilim daha büyük bir eğilimin parçası: Entelektüalizm karşıtlığının yükselişi. 7 Her türlü uzmana ve uzmanlığa olan inanç azaldı. 2018-2020'deki anketler, "uzmanlara olan inancın" tek hanelere düştüğünü gösterdi ve rakamlar o zamandan beri sadece biraz toparlandı. Birçok insan artık nesnel bilgi fikrini seçkinci olarak görüyor. 8 Giderek, "uzmanlık" fikri yerini "herkesin kendi bakış açısına sahip olduğu" algısına, Nietzsche'nin perspektifin her şey olduğu fikrine bıraktı. 9

Genel olarak konuşursak, gerçeklere ve bilgiye inanmaya yönelik bu meydan okumalar daha derin bir şeyin belirtisidir: Kolektif yönetim kurumlarının ve sosyal sermayenin postmodern yaşamı yönetme göreviyle eşit olmadığını kanıtlayan bir duygu. Güvenilemeyecek kadar büyük, kişisellikten uzak, fazla bürokratikler. Postmodern toplum o kadar karmaşık hale geldi ki, hiç kimse onun bir parçasını bile anlayamaz ve ortaya çıkan huzursuzluk, kamu kurumlarına bir tür rahatsızlık olarak yansır.

7 Tom Nichols, “Amerika Uzmanlığa İnancını Nasıl Kaybetti”, *Foreign Affairs*, Mart-Nisan 2017b.

8 Lewandowsky, Ecker ve Cook, 2017, s. 354.

9 Lewandowsky, Ecker ve Cook, 2017, s. 356.

hayal kırıklığı ve bazı durumlarda öfke. Güven, bir güvenlik duygusuna ve bir miktar paylaşılan hakikate ^{dayanır}¹⁰ ve bu şeyler azaldıkça, sosyal güven seviyeleri de azaldı. Daha doğrusu, yerel şeylere (komşulara, işletmelere ve okul kurullarına) duyulan güven ile ulusal veya uluslararası kurumlar arasındaki uçurum patladı. Amerika Birleşik Devletleri'nde ölçülebilir kaygı seviyeleri 2000'lerin başından beri istikrarlı bir yükselişte.

Sanal ve Buluş Gerçekliğin Geleceği

Gerçekliğin ölümü, son beş ila yedi yıl içinde, teknolojinin kritik bir alanındaki şaşırtıcı gelişmelerin patlamasıyla ebe oldu: gerçekçi ses ve video ve “gerçek” arasındaki sınırları bulanıklaştırmaya devam eden ilgili sahte teknolojiler (doğrulanabilir) ve icat edilmiş içerik. ¹¹ İnsanlar on yıllardır kopyalar ve sahte içerik üretiyorlar, ancak şimdi aradaki fark, ister görüntüler, ister ses klipleri veya videolar olsun, bu sahte ürünlerin o kadar yüksek doğrulukta olması ki, herhangi birinin gerçekliğini zaman olmadan doğrulamasını neredeyse imkansız hale getiriyor. tüketen ve bazı durumlarda çok kapsamlı araştırma. ¹² Aynı teknolojiler, gelişmiş robotik ve yapay zeka ile birleştiğinde, insansı robotların uzun zamandır beklenen geleceğine giden çizgiyi henüz aşmaya başlıyor, ancak şimdi bile bu eşiğin anlamlı bir şekilde aşılması gerekiyor.

İlk ortaya çıkan basit görüntü oluşturma oldu. “Photoshop” teriminin kendisi, hareketsiz bir görüntünün taklit edilmesini veya değiştirilmesini ifade eden evrensel bir terim haline geldi. 2025'te, bazıları makine öğrenimi süreçleri tarafından yönlendirilen programlar o kadar iyi ki, sahtekarlar neredeyse istedikleri her şeyin görüntülerini sesli komutla birleştirebilir. ¹³ 2015 gibi uzun bir süre önce, Reddit web sitesi resimde yarışmalara ev sahipliği yapıyordu.

10 Simon Sinek'in National Public Radio, “Trust and Consequences,” *TED Radio Hour* , 15 Mayıs 2015 tarihli tartışmasına bakın.

11 “Sahte Haber: Henüz Hiçbir Şey Görmediniz,” 2017.

12 Kevin Roose, “İşte Sahte Videolar da Gelsin,” *New York Times* , 4 Mart 2018.

13 Vincent, 2016; Karras ve diğerleri, 2018; Grigoris, 2017; Zhang ve diğerleri, 2017.

manipölasyon, hareketsiz bir fotoğrafta sahte gerçeklik yaratma konusunda en etkileyici yetenek için ödüller veriyor. 2018 yılına gelindiğinde, resimlerin doğruluğunu oluşturmak ve ardından test etmek için rekabetçi AI programlarını kullanan en gelişmiş yapay görüntü oluşturma programları, gerçek fotoğraflardan tamamen ayırt edilemeyen tamamen kurgusal insanların yüksek çözünürlüklü görüntülerini oluştuyordu. ¹⁴ Görüntülerin aslına uygunluğu artık 2018'deki üst düzey dijital kameraların çözünürlüğüyle eşleşiyor.

İnsanlar artık istedikleri kadar başka görüntüden öğeleri entegre ederek istedikleri kadar sıfırdan görüntüler oluşturabilirler. Stok görsellerde uzmanlaşan firmalar hızla harekete geçti: Görüntü üretimiyle ilgilenen kişiler, manipüle edilebilir dosyalardan oluşan devasa veritabanları satın alabilir ve beğendikleri bileşenleri çağırıp bunları nihai görüntüde bir araya getirebilirler. Ve süreç kolaylıkla otomatikleştirilebilir: AI ile görüntü oluşturma programları, kullanıcının ihtiyaç duyduğu türden çok sayıda görüntü üretmek için kullanılabilir.

Binlerce şaka ve ciddi sahtekar fotoğraf interneti doldurmaya başladı bile. 2021'de yayınlanan ve Federal Soruşturma Bürosu (FBI) gözetimi tarafından John F. Ken-nedy'nin Marilyn Monroe ile samimi bir ortamda çekilmiş olduğu anlaşılan sahte sahte görüntüler gibi bazı görüntüler tarihidir. Ulusal liderlerin fahişelerle, uyuşturucu kullanan veya çocuklarını istismar eden görüntüleri gibi, diğerleri açıkça itibarsızlaştırmak için tasarlanmıştır.

Diğer bir köklü alan ise dijital sestir, çünkü teknoloji en uzun süredir geliştirilmekte ve teknolojik olarak taklit edilmesi en kolay olanıdır. ¹⁵ Adobe'nin VoCo sistemi en iyi bilinenlerden biriydi, ancak buna Lyre-bird ve VivoText gibi bir düzine başka program katıldı. ¹⁶ Bir kullanıcının tek ihtiyacı, hedef kişinin 20 dakikaya kadar (veya bir ya da iki dakikaya kadar) yüksek kaliteli bir ses kaydıdır ve bu kişi, sesin her şeyi söylemek üzere programlanabilen dijital bir kopyasını oluşturabilir. kullanıcı beğenir. Sonuç sadece

¹⁴ Cade Metz ve Keith Collins, "How an AI 'Cat-and-Mouse Game' Inanılmaz Sahte Fotoğraflar Üretiyor," *New York Times*, 2 Ocak 2018.

¹⁵ Selçuk, 2017.

¹⁶ "Deneyisel Olalım: Adobe MAX Sneaks'in Arkasında" 2016; Adobe Inc., 2016; "İnsanların Konuşma Kalıplarını Tam Olarak Taklit Etmek Sorun Getirebilir" 2017.

dijital dosyaların karmaşık analizi ile “gerçek” bir kayıttan ayırt edilebilir.¹⁷

Bu ses platformlarının en bilinenlerinden biri Lyrebird.¹⁸ 2019'da, üç lise öğrencisinin, ABD başkanının arka plan alkışları ve sanal bir kongre izleyicisinden gelen ses efektleriyle tamamlanan paralel bir Birlik Durumu Konuşması oluşturmak için bunu kullandığı ve çeşitli bloglarda yayınladığı zaman ünlü oldu. Gönderiler bir hafta içinde 35 milyon görüntüleme topladı ve daha sonra yapılan anketler, bu sahte haberleri duyan Amerikalıların yüzde 30 ila yüzde 40'ının gerçek konuşmayı dinlediklerine inandığını ileri sürdü.

2020 itibarıyla, dijital ses üretimine yüksek kaliteli dijital video eşlik etti. Alanın kökenleri, Hollywood'da *Avatar* ve *Maymunlar Cehennemi* gibi filmlerde kullanılan ve bir oyuncunun ifadelerini dijital olarak yaratılmış bir karaktere dönüştüren dijital yakalama teknolojilerinde yatıyordu. Karakter ve ortamın giderek daha gerçekçi temsillerini arayan video oyunu endüstrisi tarafından da önemli çalışmalar yapıldı. Güney Kaliforniya Üniversitesi Karma Gerçeklik Laboratuvarı ve CGI stüdyoları gibi araştırmacılar, gerçek insanların dijital temsillerini oluşturmak için teknolojiyi kullandılar ve ardından ortaya çıkan programı istediklerini söyleyecek ve yapacak kadar esnek hale getirdiler.

2017'de bile, teknolojinin ilkel versiyonları, birkaç ulusal liderin bariz şekilde sahte - ama yine de şok edici derecede iyi - sanal versiyonlarını oluşturmak için kullanıldı.¹⁹ 2020'ye gelindiğinde, birkaç program, kullanıcıların kelimeleri veya cümleleri basitçe girebilecekleri güvenilir bir işlevi birleştirmeye başladı (“kedi kutuya atlıyor”) ve sistem böyle bir sahneyi anlatan yüksek kaliteli dijital video üretecekti.²⁰

Giderek artan bir şekilde, sanal görüntü, ses ve video oluşturma alanı, esasen, sahteleri aramak için bir AI sistemini programlamayı ve zorlamayı içeren GAN'lar biçimindeki makine öğrenimi tarafından yönlendiriliyor.

¹⁷ Fiyat, 2017.

¹⁸ Gholipour, 2017; Lyrebird, tarihsiz.

¹⁹ Garip, 2016; Thies ve diğerleri, 2016; Langston, 2017.

²⁰ Li ve diğerleri, 2018; Cai ve diğerleri, 2018.

taklit etmeye çalışmak için ikinci bir program. ²¹ Bu tür sistemlerdeki eylem-tepki yinelenmesi, insan programcılarının üretilen videonun aslına uygunluğunu artırabildiği hızı büyük ölçüde aşıyor. 2021 yılına gelindiğinde, bu tür çabalar, insanların yüzde 95'inden fazlasının görsel olarak gerçeklikten ayırt edemediği görüntüler üretme eşliğini geçmişti. GAN sistemleri, insan algısını kandırma görevini aştı ve yalnızca, birçok durumda yapabildikleri yüksek kaliteli dijital adli tıp bilgilerini taklit etmek için çalışıyor. Bu tür ilerlemeler nedeniyle, dijital sahteciliği hedefleyenlerin tek ihtiyacı, amaçlanan hedeflerin bir veya iki saatlik videosudur ve istedikleri zaman manipüle edilebilecek bir dijital temsil oluşturmak için piyasadaki en büyük ticari programlardan birini kullanabilirler. ve *Zelig* benzeri, mevcut sahnelerle düştü. ²²

Sonuçların bazıları iyi huylu olmuştur. İnsanların artık bir ücret ödeyip istedikleri zaman Margot Robbie ile istedikleri zaman, hayır kurumlarına bağışlanan ücretin geliri ile doğal olarak konuşan dijital bir replika ile görüntülü sohbet ederek sohbet edebilmeleri, sadece bir merak. James Franco'nun mobil hologramı bir Target'ta müşterilerin yanında ilk kez görüldüğünde, onlara isimleriyle hitap ederek ve onlar hakkında devasa çevrimiçi veritabanlarına erişerek kişisel terimlerle konuştuğunda, büyüklü görünüyordu ve satışlarda bir artışa neden oldu; birkaç ay içinde, insanlar bu tür bariz satıcılığı büyük ölçüde görmezden geldiler. Bir dizi genç film yapımcısı, esasen bodrumlarında, istedikleri gibi karakterler üretip manipüle ederek, elektronik müziğin dijital video eşdeğeri olan bütün filmleri yaratma yeteneği ile güçlendirildi.

Bununla birlikte, bu görünüşte büyüklü teknolojilerin diğer uygulamaları, icat edilmiş gerçekleri gerçeklerin yerine koyarak, zarar ve kaos yaratmak için tasarlanmıştır. İnsanlar artık yapmak istedikleri herhangi bir iddia için görünüşte ikna edici kanıtlar üretebilirler: tarihsel komplo teorileri, siyasi liderlerin güvenilirliğine yönelik saldırılar veya dünya olaylarının oluşumları. Küresel ısınma şüpheci, buzulların erimediğini “kanıtlayan” bir video yayınlıyor. Gerçek kanıtlardan yoksun insan hakları aktivistleri, halk arasında öfkeyi ateşlemek için toplu soykırımın sahte ses ve videosunu ürettiler. Çoğu durumda sorun, sanki

²¹ Metz ve Collins, 2018; Şeyh, 2017.

²² Simon Adler, “Son Dakika Haberleri”, *Radiolab*, 27 Temmuz 2017'de sahte ürünlerle ilgili tartışmaya bakın.

Tespit edilecek tanımlanabilir bir gerçeklik yok, ancak birçok konuda Amerikalıların üçte biri veya daha fazlasının, beklentileriyle örtüşen çarpık bir gerçeklik için çok daha güçlü bir *iştahı var ve bu yeni teknolojiler, motive edilmiş akıl yürütmeyi güçlendirdi*. benzeri görülmemiş şekillerde.

En uğursuz entrikalardan biri, 2024'te, 11 Eylül saldırılarının gerçekten de ABD hükümetinin bir komplosu olduğuna dair "kanıt" ortaya çıkarmak için -yabancı bir hükümet tarafından planlandığına inanılan- muazzam, koordineli çabayla ortaya çıktı. Komplo teorisyenleri. Sahte kanıtlar arasında çok gizli ABD Savunma Bakanlığı notları, dönemin Savunma Bakanı Donald Rumsfeld'in Başkan Yardımcısı Richard Cheney ile komplo hakkında "konuştuğu" ses kayıtları, Pentagon'u vuran sözde füzenin video görüntüleri ve daha fazlası yer alıyordu. daha fazla. Birkaç alternatif sağ web sitesi tarafından "11 Eylül'ün Pentagon Belgeleri" olarak adlandırılan bilgi akışı, sorunun süzülmesini sağlamak için daha fazla sözde yayımla devam etti. Bu tür sahtekarlıkların maskesini düşürmeye adanmış web sitelerinin iddiaları çürütmek için hemen sahte tespit yazılımları kullanmasına rağmen, anketler Amerikalıların üçte birinin artık ya iddialara inandığını ya da saldırıları kimin başlattığı konusunda "ciddi soruları" olduğunu gösteriyor.

İlgili bir sorun, bu tür dijital sahtekarlıkların oluşturulmasının artık otomatikleştirilmiş olmasıdır. İçerik oluşturucular yıllardır otomatik içerik oluşturmak için yapay zekayı kullandılar, ²³ ancak çok daha yetenekli yapay zeka ile birinci sınıf dijital üretim tekniklerinin evliliği, tamamen yapay olarak oluşturulmuş bir görüntü, ses ve video patlamasına yol açtı. Elektronik müziğin çoğu artık herhangi bir insanın (müzisyen, yapımcı veya şarkıcı olmadan) katılımı olmadan AI tarafından yaratılıyor ve bu model giderek orkestra, pop ve rock türlerine yayılıyor. ²⁴ Çoğu televizyon reklamı, herhangi bir insan aktör olmadan bu şekilde oluşturulur;

²³ Matt Chessen, *The MADCOM Future*, Washington, DC: Atlantik Konseyi, 2017b.

²⁴ Caz dinleyicileri, dijital jenerasyonun doğasında var olan yapaylığı reddederek, 2023 yılına kadar, ilk olarak "The Fusion Collective" adlı bir insan grubuna atfedilen avangard caz albümü "Waterfront Lullaby"nin piyasaya sürülmesiyle, yıllarca direndi. " ve *The Jazz Review* tarafından hızlı bir şekilde "yeni bir klasik, daha fazla olmasa da on yılda türün en büyük ifadesi - ve eğer birinin ihtiyacı varsa, insan sezgisine, zanaatına ihtiyacımız olduğuna dair daha fazla kanıt ve evet, gerçek cazın yaratılmasının ardındaki ruh ." "The Fusion Collective"nin bir şirket olduğu ortaya çıktığında

tüm basılı reklamlar yapay zeka tarafından oluşturulur. 2024'te, tamamen bir bilgisayarda oluşturulmuş, sinemalarda gösterime giren ilk büyük sinema filmi ortaya çıktı. Yeterince uygun bir şekilde, devasa bir merkezi bilgi sinir sistemine bağlı gelecekteki bir toplum hakkında bir bilim kurgu hikayesiydi. Gerçek aktörlerin (hakları satın alınan) görüntülerinin ve tamamen kurgusal birkaç dijital yaratımın bir kombinasyonunu oynadı. Yapılması yaklaşık 18 milyon dolara mal oldu - gerçek, fiziksel filmlerin maliyetine göre doların on senti.

25

Bu teknolojilere karşı koyma ve insanların gerçek görüntüleri sahte olanlardan ayırt edebileceklerine dair daha güçlü bir algıyı yeniden tesis etme çabaları birkaç yıldır devam ediyor. ABD Savunma Bakanlığı, görüntüleri değerlendirmek ve fabrikasyon videoları ortaya çıkarmak için yapay zeka kullanan çalışmalara sponsor oldu. 26 Bu sistemler, insanların gözlerini kırpmadığı videoları aramak gibi basit pratik kurallar kullanarak erken nesil video üretimlerini yakalamada bir dereceye kadar doğruluk sağladı. Ancak, bazıları devlet destekli olan sahtekarlar, kolayca tespit edilebilen sahteciliğin önceki sürümlerini çok daha karmaşık, AI destekli tekniklere taşıdılar. Ve mevcut yazılım filtreleri teorik olarak doğruluğun belirlenmesine yardımcı olabilirken, çoğu insan bunları kullanmaz ve nüfusun önceden belirlenmiş inançlarıyla uyumlu olan sahte video ve ses dosyaları kolayca çürütülse de geniş çapta kabul edilir. Bu tür sahte kalıplar, temel gerçeklerle kurulan eğilimi böylece devam ettirdi: Doğrudan düzeltme yoluyla karşılanabilecek ve karşılanması gereken geçersiz iddialar, nüfusun önemli bir bölümünü hala ikna edebilir.

Bu görüntü, işitsel ve görsel sahtecilik teknolojileri paralel olarak gelişti ve günümüzde büyük ölçüde birleşti.

Amazon sponsorluğunda, caz üreten Marsalis adlı yeni yapay zeka programında, birçok caz dinleyicisi omuz silkti ve bir sonraki albümünü satın aldı. "Waterfront Lullaby"den 96 saat sonra çıktı.

25 Filmde rol alan icat edilmiş "aktörlerden" biri olan Aiden Williams, filmin vizyona girmesinden sonraki yıl içinde 40'tan fazla reklamda yer alarak kısa sürede en çok kazanan ünlülerden biri oldu.

26 Will Knight, "ABD Ordusu Deepfakes ve Diğer Yapay Zeka Hilelerini Yakalama Çabasını Finanse Ediyor," *MIT Technology Review*, 23 Mayıs 2018a; Will Knight, "Savunma Bakanlığı Derin Sahteleri Yakalamak İçin İlk Araçları Üretti," *MIT Technology Review*, 7 Ağustos 2018d.

iki ilgili alan: VR ve AR. Örneğin, ortaya çıkan AR uygulamalarında, insanlar günlük yaşamlarından geçerken, nesnelere ilişkin algıları benzeri görülmemiş şekillerde küratörlüğünü yapıyor. Ofislerinin görünümü ve içeriği, sokaktan geçen insanların görünümü ve çevredeki reklamlar da dahil olmak üzere her şey özelleştirilebilir ve özelleştirilebilir hale geldi. ²⁷ Nesnelerin algılanan kalitesindeki bu tür sürekli değişiklik, paylaşılan bir sosyal deneyimin hakimiyetini zayıflatma eğiliminde olmuştur. Temel olarak tüm insani toplumsal varoluş olarak kabul ettiğimiz birçok yönden, böyle bir ortak nesnel deneyim artık var olmayacak. İnsanlar dünyayı tam anlamıyla bir dizi kendi kendine programlanmış filtre aracılığıyla görecekler.

İnsanlar artık kendilerine getirilen her şeyi özünde gerçekmiş gibi deneyimliyorlar. AR destekli eğlence karakterleri ve haber öyküleri ile başladı, ²⁸ ve bir kişinin akıllı telefon ekranını veya AR kulaklığını doldurmak için her türlü görüntüyü sunan binlerce şirket, kuruluş ve birey örneği ile devam etti.

Son olarak, artan robotik uygulamaları, gerçek ve yapay arasındaki sınırın bulanıklaşmasına da yardımcı oluyor. Yapay zeka veya insan güdümlü çevrimiçi botlar veya fiziksel robotlar, terapi, evde bakım ve diğer etkileşimli uygulamalar için önemli yeni bir pazar oluşturur ve bunlar ayrıca çok sayıda insan hakkında daha fazla bilgi toplar. Beş yıl önce CareCoach adlı bir firma, evde bakım ortamlarında yaşlı hastaları izlemek için avatarlar kullanmaya başladı. Avatarlar, bu firmanın durumunda, dikkatle işe alınan ve iyi eğitilmiş insan operatörler tarafından yönlendirilir. Sistemler tüm gün birini izleyebilir ve düzinelerce bilgiden haberdar olabilir ve müşterilerle güçlü kişisel bağlar kurabilir. Birçoğu küçük köpekleri veya diğer avatarları yakın arkadaşlar olarak görmeye ve sohbetle devam etmek için onları yürüyüşlere veya tekne gezilerine götürmeye geldi. ²⁹ İnsan ve yapay ilişkiler arasındaki çizgi giderek belirsizleşiyor.

²⁷ David Pierce, "Enjoy Your New Virtual Office," *Wired*, Şubat 2018, s. 43.

²⁸ Graham Roberts, "Artırılmış Gerçeklik: Haberleri Evinize Nasıl Getireceğiz," *New York Times*, 1 Şubat 2018.

²⁹ Lauren Smiley, "Something To Watch Over Me," *Wired*, Ocak 2018.

Dünyanın Paylaşılan Bir Resminin Sonu

Bütün bunların sonucu, büyük sosyal konularda genel olarak kabul edilen bir dizi gerçek gibi herhangi bir şeye halkın bağlılığının azalması oldu.

Tüm “gerçekler” ortadan kaybolmuyor veya alakasız hale gelmiyor. Bazı yavan, bilimsel temelli ve kişisel olarak onaylanmış gerçekler varlığını sürdürüyor. Bakterilerin hala enfeksiyonlara neden olduğu anlaşılakta ve antibiyotiklerle tedavi edilmektedir. Mühendisler hala yeni bir ev veya köprü için destek gereksinimlerini hesaplayabilirler.

Yine de, gerçeğin sözde bilimsel değerlendirmeleri alanında bile, giderek daha fazla konu tartışılıyor. İklim değişikliği ve aşılarda üzerindeki tartışmalar belki de önde gelen örneklerdir ve çoğu Amerikalı, yankı odalarının algıları dışında her iki alanda da anlamlı bir gerçeklikten artık emin değildir. Bu eğilim, toplumdaki suç düzeyi, eğlence amaçlı uyuşturucuların oluşturduğu sağlık tehdidi ve çeşitli hastalıklara yönelik tedavilerin güvenilirliği gibi nesnel bir anlaşmaya varılması gereken diğer konulara da yayılmıştır. Bu ve diğer durumlarda, karanlık kampanyalar, herhangi bir fikir birliği potansiyelini baltalamak için çeşitli dezenformasyon ve sahtekarlık araçları kullandı. Sonuç, hükümetin politika tepkilerini felç etmek oldu.

İnsanların çözmek ve onlar hakkında yargıda bulunmak için kullanabilecekleri nesnel bilgilerin temeli sorgulandığından, çekişme halindeki büyük sosyal ve politik meseleler için zorluk daha da şiddetlidir. Bu nedenle gerçek eğilim, gerçeğin ölümünden daha spesifiktir: Şimdi sorun , *büyük kavramın anlamının sosyal meseleler ve olaylar giderek daha belirsiz hale geliyor* . İkisinden biri aşılarda, iklim değişikliği, suç, belirli ekonomik politikaların etkileri veya diğer yüzlerce konu hakkındaki sorularda, siyasi yapı içindeki genel yargıları desteklemek için üzerinde anlaşmaya varılan herhangi bir gerçek üzerinde anlaşmak giderek imkansız hale geliyor.

Gerçeğe duyulan ilginin azalması kadar, çağ, 4chan topluluğunda ve hiçbir şeyi ciddiye almayı reddeden diğer çevrimiçi topluluklarda uzun süredir yerleşik olan alaycı, katı ironi türünde bir patlamayı temsil ediyor. Giderek artan bir şekilde, çevrimiçi estetik, parodi, şakacılık ve yerleşik değerleri ve kurumları yıkmak için tasarlanmış kapsamlı bir uyumsuz alaycılık ruhudur.

dersler. ³⁰ Bu tür topluluklardaki en büyük günahlar, herhangi bir şeyi olduğu gibi kabul etmek, herhangi bir şey için müesses nizamın sözünü almak veya herhangi bir değeri veya geleneği ciddiye almaktır. Çağın karakteri, gerçeğin ölümünün çok ötesine geçti: amansız bir ironinin saldırısı altında anlamın ya da paylaşılan anlamın ölümü.

Gerçekten de, bir sosyal norm olarak dürüstlüğü değeri, bilgi ortamının önemini küçümsemeye çok kararlı görüldüğü için artan bir stres altına girmiştir. *Wired* dergisinin 2018'de önerdiği "hacker's Creed", uzun zamandır "[e]aydınlatmalı hile, en yüksek oyun şeklidir." İtaatsizlik, bir değer olarak uyumun önüne geçer. ³¹ Ortaya çıkan bu inanç sistemi, özellikle teknik ve bilgi ile ilgili alanlarda giderek daha yaygın hale geldi.

Bu eğilimlere karşı bir isyanın ilk parıltıları, insanlar gerçekliğe susamış ve bir post-gerçeklik dünyasının icat edilmiş sahtekarlığına karşı bir isyan ifade etmeye başladığından, onlarca yıldır sürüyor. Daha 1980'lere gelindiğinde, ABD edebiyatındaki önemli gerilimler, "alışveriş merkezi kültürü ve kitle iletişim araçları tarafından bombardımana tutulan", "hayatlarından çok 'McLive'ları' olduğuna" inanmaya başlayan insanlarla ilgili bir huzursuzluğu yansıtıyordu. ³² Otantik işaretlere duyulan arzu -zanaat temelli işletmeler, kırsal yaşam ve kütük evler, "şebekeden uzak", doğal ve organik yiyecekler ve çok daha fazlası için - şimdi özellikle genç Amerikalılar arasında önemli bir tema. Ancak yeni çağın bilgi özelliklerindeki temel eğilimleri durdurmadı.

Gerçekliğin Ölümünde Bilgi Saldırganlığı ve Manipülasyonu

Bu eğilimler ve gerçekler ortaya çıktıkça, enformasyona dayalı saldırıların belirli biçimleri "öğrencilerin ölümünü" karakterize etmeye başladı.

³⁰ 2017 itibarıyla trend hakkında bir tartışma için bkz. Angela Nagle, *Kill All Normies: Online Cul-ture Wars from 4chan and Tumblr to Trump and the Alt-Right*, Winchester, Birleşik Krallık: Zero Books, 2017, özellikle s. 5-7 ve 28-29.

³¹ Virginia Heffernan, "Twilight of the Hacker" *Wired*, Şubat 2018, s. 14.

³² Kalkanlar, 2010, s. 25.

gerçeklik.” En önemlisi, bir yorumcunun 2018'de ³³te belirttiği gibi hızlanan “ortak bir kamusal gerçekliğin çöküşü”, manipülatörlerin belirli sektörler arasında algılar yaratmak için bu giderek sanallaşan, hayal edilen, postmodern manzarada çalışması için fırsatlar yarattı. nüfusun. Ve bunu yapmak için daha etkili araçlara sahipler, ses, video, durağan görüntüler ve hemen hemen istedikleri her şeyi büyük bir doğrulukla gösteren VR programları üretme becerisine sahipler. Kodu manipüle etmek artık bir bilgisayar sisteminin işleyişini bozmakla ilgili değil; insanların karşılaştığı gerçekliğin doğasını değiştirmekle ilgilidir.

Yaklaşık 2021-2022'ye gelindiğinde, seçimlerden veya referandumlardan önceki haftalarda ileri demokrasilerin siyasi manzarasında çok sayıda kışkırtıcı görüntü, video ve ses "kayıtının" uçması olağan hale gelmişti. Politikacılar rüşvet alırken veya ilişki kurarken "görülüyordu", nüfusun büyük gruplarına hakaretler duyuyorlardı ve organize suç veya düşman dış güçlerden gelen rakamlarla gizli anlaşma içinde gösteriliyorlardı. Siyasi liderler, "saygın" haber kaynakları ve diğerleri bu saldırılara karşı koymak için çok çalıştılar, ancak çabaları her zaman eksik ve bazen bir fark yaratmak için çok geç: Nitelikli manipülatörler saldırılarını bir seçimin veya oylamanın eşiğinde nasıl zamanlayacaklarını biliyorlar. . Pek çok durumda, politikacılar bu tür saldırılarla itibarsızlaştırıldı; birkaç seçim açıkça etkilenmiştir.

Aynı zamanda, manipülatörler, hedef ülkelerdeki ortak bir sosyal gerçeklik potansiyelini yok ederek bu saldırılara verilen yanıtları önceden almak için çok çalışıyorlar. Gerçek kontrol web sitelerinin ve diğer “nesnel” web tabanlı bilgi kaynaklarının etkilerine karşı koymak için, web'deki nesnel bilgileri alt etmek için dinamik olarak oluşturulmuş içerik üretmek için yapay zekayı kullanıyorlar. Ayrıca, Wikipedia sayfaları gibi çevrimiçi kaynakları aktif olarak şekillendiriyor ve yanlış hikayeleri yerleştirmek için bazı nesnel siteleri doğrudan hackliyorlar. (Rezil bir vakada, *Financial Times* web sayfası, bir İngiliz politikacının mali durumu hakkında dikilmiş, tamamen uydurma bir hikaye yayınladı.

33 John A. Gans., Jr., “Governing Fantasyland,” *Survival* , Vol. 60, Sayı 3, Haziran-Temmuz 2018, s. 200.

kabahatler. Politikacı bunu öğrenip gazete editörlerinin dikkatine sunmadan önce iki gün geçmişti.)

Algılanan gerçekliği sosyal medya aracılığıyla şekillendirmeye yönelik çabalar, son yıllarda turbo şarjlı hale geldi. Yapay zeka güdümlü botlar artık bu platformlardaki rekabeti domine ediyor; telafi edici pozisyonları tespit edebilir ve büyük ölçüde insanlardan ayırt edilemeyen şekillerde yanıt olarak tartışabilirler. Büyük veri hırsızlığı ve düşman güçler tarafından bireysel Amerikalılar (ve daha az ölçüde Avrupalılar) hakkında Facebook veya Google boyutunda veritabanlarının kurulmasıyla birleştiğinde, Moskova veya Pekin'deki bir bilgi saldırganı artık reklamları, mesajları ve bilgileri tam olarak hedefleyebilir. herhangi bir platform şirketi. Son raporlar, Çin'in on binlerce yüksek eğitilmiş, sosyal medya konusunda bilgili, İngilizce konuşan trolleri, ABD kamuoyunda algıları değiştirme ve belirli davranışsal sonuçlara ulaşma açısından belirli hedeflere sahip kalıcı, devam eden bir kampanyaya adanmış olduğunu gösteriyor.

Çoğu zaman bu tür kampanyaların amacı, insanları belirli bir anlatıya inandırmak değil, var olan inanç sistemlerini beslemek ve yabancılaşmayı, öfkeyi ve çatışmayı hızlandırmaktır. Saldırganlar, uç grupların en paranoyak içgüdülerine hitap etmek ve genel olarak siyasi kutuplaşmayı sertleştirmek için tasarlanmış videolar üretiyor. Cumhuriyetçiler, Demokrat politikacıların korkunç şeyler söylediğini ve yaptığını gösteren sürekli bir doz video alıyor; Demokratlar, Cumhuriyetçi politikacıların benzer videolarını alıyor.

Bilginin doğruluğunu ve akışını etkilemenin ötesinde, bilgi saldırganları, Amerikalıların günlük yaşamlarında karşı karşıya kaldıkları, giderek daha fazla yaratılan gerçekliğin parçalarının kontrolünü ele geçirmenin yollarını giderek daha fazla deniyorlar. Askeri travma sonrası stres bozukluğu (PTSD) hastalarına hizmet eden ve ters tepme tavsiyeleri veren sohbet robotlarını hackleyen manipülatörlerin doğrulanmış vakaları var. Birkaç durumda, sofistike bilgisayar korsanlarının VR akışlarını değiştirmeye başladığı, VR kulaklıklarında oynanan video oyunlarındaki olayları biraz değiştirdiği görülüyor; kışkırtıcı ses yerleştirmek için sanal gerçeklik tarafından barındırılan iş yeri tartışmalarına girmek; veya cep telefonlarındaki AR uygulamalarına rahatsız edici görüntüler eklemek. Giderek yaygınlaşan bir taktik, erişebilecekleri herhangi bir VR veya AR akışlarına bilinçaltı mesajları eklemek gibi görünüyor.

Gerçekliğe yönelik bu ısrarlı saldırının etkileri daha yeni hissedilmeye başlandı, ancak şimdiden demokrasi için zaten sorunlu olan bilgi küresinin zorlu yönlerini daha da kötüleştiriyor gibi görünüyor. Pek çok ileri demokrasi, üretken politika oluşturmak için çok az zamanları veya enerjileri kaldığı için “gerçeği” desteklemeye takıntılı hale geldi. Bu saldırılar, reform ve değişim konusunda iki taraflı yeni bir fikir birliğinin yaratılmasını neredeyse imkansız kılacak şekilde demokratik toplumların kutuplaşmasını derinleştiriyor.

Özellikle zararlı olduğu ortaya çıkan şey, bu durumu iyileştirmeye yardımcı olmak için ayaklanan bireyleri veya grupları itibarsızlaştırma alışkanlığıdır. Yeni doğrulama grupları ortaya çıktığında, bunların bazı kötü suçlularla bağlantılı olduklarına, partizan bağışlarıyla finanse edildiklerine veya genel olarak yozlaşmış olduklarına dair bir düzine rapor ortaya çıkacak. Olguların doğruluğunu savunan herhangi bir politikacı, özellikle acımasız sanal saldırılara maruz kalıyor.

Bazı durumlarda, Amerika Birleşik Devletleri'nde, bu tür saldırıların etkinliği, temsil bölgelerinin ve eyaletlerin uzun vadeli gerry manipülasyonu ve kutuplaşması süreci tarafından desteklenmiş ve teşvik edilmiştir. Artık birçok temsilci, özellikle ön seçimlerde, orantısız bir şekilde nüfusun dar kesimlerinin görevde kalmasına güveniyor. Manipülatörler, bu dilimlerin algılarını bir bütün olarak popülasyondan daha etkili bir şekilde etkileyebilir. Bu etki, tek bir ideolojik alt grubun egemenliğine giren ve siyasi eylem üzerinde genel bir caydırıcı etkiye sahip olan ve çoğu liderin boyun eğmek istemeyen bir siyasi partiden farklı değildir.

En genel olarak, bu saldırılar, demokratik olsun ya da olmasın, her türden gelişmiş toplumun verimli çalışmasını sağlayan temel yapıstırıcı olan sosyal güveni daha da aşındırıyor. Medyadan hükümete, sosyal gerçekliğin aracı kurumları, 2018 yılına kadar güvende önemli bir düşüş yaşadı. Artık güvenilir bir nesnel gerçeklik fikri gerçek tehlikede. Belirli bireylere ve kurumlara olan güveni sarsmak için tasarlanmış bir toplumda sürekli bir uydurma saldırılar akışı yaşandığında bekleneneği gibi, bu eğilimin toplumsal güvenin diğer unsurları aracılığıyla basamaklandığına dair kanıtlar vardır. Son on yılda, nesnel, doğrulanabilir bir gerçeklik duygusunu zayıflatmaya hizmet eden uzun vadeli eğilimler, derinden etkileyen bir dizi teknolojinin etkisi altında hızlandı.

Amerika Birleşik Devletleri ve diğer gelişmiş ekonomilerin bilgi dünyası. Bireysel teknolojilerin eğiliminin ve gerekçesinin bazı nedenleri umut verici ve yaratıcıdır, ancak etkisi birçok ülkede sosyal tutarlılık ve demokratik istikrar açısından tehlikeli olmuştur. Ve trend hızlandıkça, nasıl tersine çevrilebileceği ve hatta yönetilebileceği giderek daha az netleşti. “Gerçekliğin ölümü” kendi kendini güçlendiren bir süreç gibi görünüyor; Her geçen yıl, ortak bir gerçekler ve olaylar vizyonunu yeniden onaylamak giderek daha az makul görünüyor.

Gelecek 2: İnanç Siloları (2024 Senaryosu)

Genel Gelecek

Yıl 2024 ve insanlar her zamankinden daha fazla kapalı, karşılıklı olarak şüpheli bilgi ortamlarına çekildiler. Aynı ülkedeki birden fazla insan grubu artık esasen farklı gerçekliklerde yaşıyor.

Zamanla, insanların kendilerini sıkı bir şekilde kendine referans veren bilgi topluluklarına kapatma yetenekleri ve eğilimleri sadece hızlandı. Ağ haberleri, büyük günlük gazeteler ve siyasi liderlerden oluşan iki taraflı bir çekirdek gibi paylaşılan gerçek ve anlam kaynakları olarak hizmet eden yayınlar, yerini daha ayırık, ısmarlama ve genellikle partizan bilgi kaynaklarına bırakmaya devam etti. . Bu değişim, kısmen değişen ekonominin ve saygın bilgi filtrelerinin sürekli köretilmesinin bir işlevi olmuştur. Bu eğilimin yakın tarihli bir örneğinde, *Washington Post* sahibi Jeff Bezos, gazetenin iş modelinin “geri alınamaz” olduğunu ve faaliyetlerini yılda on milyonlarca dolarla sübvansede etmeye devam edemeyeceğini ilan etti. Gazetenin personeli, yalnızca çevrimiçi bir formata geçiş yapmak ve raporlama personelinin boyutunu küçültmek için bir plan geliştirdi, bu da daha az hikaye ve ayda yalnızca bir veya iki araştırma raporu akışıyla sonuçlandı.

Ancak gazetenin editörleri aynı zamanda çağın ruhunu yansıtan çok önemli bir karar da verdiler: Birkaç yıl boyunca genel bir okuyucu kitlesine büyük ölçüde başarısız olan bir çekicilikten sonra, bu ünlü büyük günlük gazete şimdi kendisini “düşünceli ilerici için temel rehber” olarak faturalandırıyor. Çeşitli inanç gruplarından insanları bir araya getirmek yerine, kendisini tek bir mega siloda baskın oyuncu yapmaya çalışarak, açıkça belirli bir demografiye hitap ediyor. Bu uygulama artık içerik oluşturma için bir normdur.

her çeşitten aktörler. Oyunun adı, geniş bir çekicilik kazanmak yerine bir silo bulmak ve ona bir ürün, bir bilgi kanalı veya bir bakış açısıyla hükmetmektir.

Bu eğilimler ve bu gelecek en iyi niyetlerle başladı. İnsanlar, hobileri, meslekleri veya endişeleri ile ilgili olarak, tartışma ve paylaşılan fikirler için benzer ilgi alanlarına sahip kişileri arıyorlardı. Ortak öneme sahip konularda harekete geçmek için benzer fikirlere sahip olanlarla uyum sağlamaya çalıştılar. Bu tür sanal toplulukların, bireysel kimlikleri soyut kalıplara ve eğilimlere batırma riskini taşıyan kitlesel, genellikle homojen toplumlar çağında insanların aidiyet ve ontolojik güvenlik duygularını desteklemede önemli oldukları kanıtlanmıştır. İnsanların benzer bireyleri aramasına izin vererek, sosyal medya platformları ve diğer etkileşim biçimleri önemli bir psikolojik güvence sağladı.

Ayrıca, bireysel ifadeyi güçlendirmenin başka bir biçimini de sundular. Bu yeteneklerle, insanlar yakın çevrelerinin kısıtlamalarını aşabilir ve benzer inanç, deneyim, tercih veya diğer ortak kimlik veya görüşlere sahip insanlarla bağlantı kurabilir. Önyargı veya baskıyla karşı karşıya kalanlar, benzer bir durumda başkalarıyla bağlantı kurabilir ve güçlendirilebilir ve desteklenebilir. İnançları toplulukları tarafından bastırılan insanlar bu yollarla destek bulabilirler.

Bilgi alanının *silolaşması* , kısmen, bireyselleşme çağının doğal sonucudur. Pazarlama kampanyaları artık neredeyse tamamen kişiselleştirildi; bir kişinin aldığı reklamlar, kendi özel taleplerine kadar bile, reklam verenlerin kullanabileceği binlerce veri noktasına göre özelleştirilir. Nüfusun geniş kesimlerine tek bir kitlesel çekicilikte hitap etme fikri, şimdi 1950'lerin sigara reklamı kadar ilkel görünüyor. Günümüzde pazarlamacılar, veritabanlarından büyük miktarda bilgi toplayan ve yüksek düzeyde uyarlanmış mesajlarla küçük gruplara veya belirli kişilere ulaşan yapay zeka destekli motorlarda düğmelere basıyor.

Ancak, modern bilgi dünyası ile ilişkili birçok eğilimde olduğu gibi, zorluk, böyle bir yeteneğin kontrolden çıkmasını ve bireysel olarak güçlendirici olmaktan ziyade sosyal olarak yıkıcı şekillerde ifade edilmesini engellemek olmuştur. Marşın parçalanması-

Dar gruplara yönelik pazarlamanın karakteristiği olan ketplace, artık politik, sosyal ve bilgisel anlamda toplum genelinde bir parçalanma ile birleştirildi.

Bireyler için bilgi erişimi açısından, insanların kendi tanımladıkları gruplar içinde faaliyet göstermeleri, basitçe kabul edilen bir yaşam biçimi haline geldi. Bunlar profesyonel, ideolojik, etnik veya başka türlü olabilir, ancak insanların kimliklerinin temel kılavuzları artık ait oldukları ayırt edici yankı odalarıdır. İnsanlar giysiler giyer, arabalarına çıkartmalar yapıştırır ve aksi takdirde bu siloların göstergeleriyle kendilerini tanımlarlar. Daha geniş topluma çok daha az bağlı olan alt gruplar halinde çalışma alışkanlığı artık sağlam bir şekilde yerleşmiştir.

Aynı teknolojiler, zamanı ve iştahı olanlar için silolarından geçmişte olduğundan daha temel bir şekilde çıkmaları için yollar *sağladı* . Bu, uzun zamandır internette yerleşik bir fırsat ve daha kapsamlı bilgi ortamı olmuştur. İnsanlar, örnek alınacak muazzam bir fikir, yaklaşım ve inanç menüsüne sahiptir. Ancak genel sonuç, yine de, insanların bilgi diyetinin kademeli olarak parçalanması oldu ve bu, toplumun en azından bir kısmının, sınırlı inanç silolarına daha da derinlere sığınmasına neden olan araya giren psikolojik ihtiyaçları ve tepkileri katalize ediyor gibi görünüyor. Örneğin bazı sosyal medya platformları, insanları haber akışları aracılığıyla algoritmik olarak belirlenmiş tercihlerinin dışından gelen tutumlara kasıtlı olarak maruz bırakmak için öneriler benimsemiştir. Kullanıcıların bir kısmı tekliften yararlanırken, deneyimler yüzde 30 ile yüzde 60 arasında (alt gruba ve zamanlamaya bağlı olarak) kabul etmediğini gösteriyor; silolarının temel inançlarına açıkça aykırı olan manşetleri görmezden geliyorlar.

Parçalanmış Bir Toplum

Bilgi silolarının varlığı, daha derin sosyal ve ekonomik eğilimler, özellikle de toplumun daha belirgin ve daha az geçirgen sınıf, bölgesel ve bazı durumlarda etnik ve ırksal kesimlere bölünmesi üzerine kuruludur. Bu bölünme, ülkede büyüyen ve enformasyonla güçlendirilen siyasi kutuplaşmanın doğal uzantısıdır.

vatandaşların esasen neye inanmak istiyorlarsa ona inanmalarına izin veren ve başka herhangi bir şeye inananları sürekli olarak itibarsızlaştıran silolar. Bu güçlü bilgi balonlarının ortaya çıkması, halihazırda sürmekte olan kutuplaşmayı derinleştirdi ve anlamlı reformların hayata geçirilmesini imkansız hale getirdi.

2023'te, sadece bir örnek olarak, büyüyen federal bütçe açığını ve borcunu ele almak için tasarlanmış bir dizi yetkilendirme programı reformunun en sonuncusu, oylama için Meclis veya Senato'ya gelmeden önce çöktü ve rakipler tarafından geri dönülmez bir şekilde paramparça edildi. Bir avuç sosyal medya bilgi girişimcisinin, mevzuatın ne üreteceği konusunda özenle seçilmiş silolarda çılgın söylentiler ve komplo teorileri yayan taban kampanyaları. Hayırseverlik için bağış toplama giderek artan bir şekilde, her zaman etnik köken, ırk, milliyet, meslek veya ilgi alanları ile ilgili olmayan, ancak giderek bir kişinin kimliğine üye olarak hitap eden silolara (bu tür dar tanımlanmış gruplardaki başkalarına yardım etmek için bağış istemek) dayanmaktadır. belirli bir grup. Temel politika konularında ulusal iki partili fikir birliği, bir anlamda, sosyal olaylar tarafından ele geçirildi: Artık mevcut değil veya ölçülebilir bir şekilde var olamaz. Herhangi bir konuda ulusal ilerleme kaydetmeyi umut eden siyasi liderler, şimdi düzinelerce silodan gelen anlaşma parçalarını bir araya getirmelidir.

Bu siloların çoğunu yöneten ortak bir tema, insanların gerçeklerine dökülen bilgi dilimlerinin son derece sansasyonel hale gelmesidir: şiddet içeren, cinsel içerikle dolu ve dedikodu ve ima üzerine kurulu. Zamanla, bilgi pazarlamacıları en çok dikkat çeken kesin insan bilgi iştahını keşfettiler. Farklı bilgi ve içerik biçimleri, insan beyni için diğerlerinden daha lezzetlidir; aşırıya ve gıcıklayıcıya karşı nörobiyolojik bir eğilimimiz var. ı Bazı insanlar bu tür içeriklerin kendi kendini güçlendiren silolarında kapana kısıldı ve bunun sonucunda binlerce kişi ciddi duygusal travma ve psikolojik yaralanma yaşadı. Ülke genelinde “travma geçirmiş bilgiler” için terapötik tedavi merkezleri ortaya çıktı.

ı Pariser, 2011, s. 14.

Birleşik bir sosyal deneyim olarak adlandırılabilen şey fikri artık moda oldu. Gençler arasında yaşlı Amerikalılar için popüler bir terim, evrensel bilgi, deneyim ve hakikat biçimlerini deneyimlemek için nostaljik bir arzuya sahip insanlara atıfta bulunan “totalist”tir. Aynı konsere katılan insanlar, ışık gösterileri, reklamlar ve hatta konuk sanatçılar eklemek için satın alabilecekleri AR gözlükleri sayesinde artık önemli ölçüde farklı deneyimlere sahipler. Daha da önemlisi, artık tüm Amerikalıların maruz kaldığı tek bir “haber” dizisi yok. Gazeteler artık neredeyse tamamen dijital ve yayınlar, web aramaları veya Netflix önerileri kadar algoritmik olarak yönlendirildi. Büyük makaleler, okuyucuların görmek *isteyebilecekleri veriler hakkında veri toplar* ve önce bu hikayeleri besler. Aynısı, artık belirli izleyicilere dikkatlerini çekecek haberleri vermek için programlanabilen AI güdümlü VR avatarları tarafından “barındırılan” televizyon haber yayınları için de geçerli oldu. ²

İlişkili bir sorun, insanların kapalı gerçekliklerde olduklarını *düşünmemeleridir*. Anketler sürekli olarak, insanların geniş bir bilgi yelpazesine eriştiklerini varsaydıklarını ve dünya ile etkileşimlerinin kör perdelerle gerçekleşme derecesini küçümsediklerini gösteriyor. Geniş bir fikir yelpazesinden ne kadar kopuk olduklarını takdir etmezler.

Ortaya çıkan bu gerçeklikte, sürü davranışının, bir bütün olarak toplumdan ziyade parçalanmış sosyal etkileşim silolarında daha yaygın olduğu ortaya çıkıyor. İnsanlar genel olarak paniğe ve sürü davranışına maruz kalır, ancak sosyal varlık ne kadar büyük ve çeşitli olursa, teorik olarak sürü akışını belirli bir yöne sınırlamak için o kadar fazla sönümleyici vardır. Ancak ideolojik, ulusal, etnik, ırksal veya politik olarak homojen bir silo içinde, hayvancılık dinamiklerinin aşırı ve kaçınılmaz olduğu kanıtlanmıştır.

² Pariser, 2011, s. 45.

Silo Savaşları

Zamanla, giderek daha fazla şüphe uyandıran bu silolar, daha geniş sosyal parçalanma ve ideolojik kutuplaşma eğilimleriyle birlikte, karşıt gruplar arasında giderek daha düşmanca bir dizi saldırgan eylem üretti. Bu eylemler arasında trolleme, siber zorbalık, kimlik hırsızlığı, dağıtılmış hizmet reddi (DDoS) saldırıları ve bir bilgisayarı veya sistemi bunaltan e-posta ve istem selleri sayılabilir. Bu savaşlar -sanal topluluklar arasında olsa da- devletleri devletlerle, devletleri devlet dışı aktörlerle ve devlet dışı grupların ağlarını benzer ağlarla karşı karşıya getirir. Milyarderler, belirli siloların inançlarını güçlendirmek için bilgileri finanse eder ve başkaları üzerinde -bazen ikna etmeyi amaçlayan, çoğu zaman kısır siber zorbalığa dönüşen- bilgi savaşlarının başlatılmasına yardımcı olur.

Savaşlar aynı zamanda gerçekler üzerindeki tartışmalara da odaklanır. Küresel ısınmaya şüpheyile bakan muhafazakar gruplar, aşı karşıtı veya genetiği değiştirilmiş organizmalar (GDO'lar) olan bazı ilerici grupların yaptığı gibi, alıcı baloncuklara sürekli olarak yanlış yönlendiren bilgiler akışı sağlıyor. Zengin bireyler veya siyasi eylem komiteleri basitçe bir şeye inanmak istediklerine karar verebilirler ve eğer bu iddia önceden var olan ideolojik inançlarla kabaca uyuyorsa, bu tür inançları teşvik etmek için -genellikle gerçek ve uydurma bir karışım- bilgi üretebilirler.

Bilgi küresinin parçalanması nedeniyle, bu kampanyaların sınırları vardır ve hiçbir zaman çoğunluk desteğine ulaşamazlar. Ama parçalanmış bir toplumun doğası öyle ki, buna gerek yok. Son yirmi yılın önemli bir dersi, iki siyasi partinin bir tikanıklık içinde olduğu oldukça kutuplaşmış bir durumda, nüfusun yüzde 30'unu bile büyük bir politika fikrine karşı harekete geçirmenin onu öldürmek için yeterli olduğudur. Bu, özellikle, bu yüzde 30'un çoğu iki partinin taban seçmenleri içinde yer alıyorsa ve bu nedenle, birincil zorluklar hakkında endişelenen seçilmiş yetkililerin kalplerine özel bir korku salıyorsa geçerlidir. Geçmişte, bu tür azınlıklar politika fikirlerine -örneğin medeni haklar reformlarına - karşı çıktıklarında, siyasi engellemeyi geçersiz kılmak için iki partili daha büyük bir çoğunluk mevcuttu. Artık durum böyle değil.

Ve bu sonuç artık bilgi baloncuklarının gerçekliği tarafından yerine kilitlendi. Herhangi bir konuda geniş bir iki partili çoğunluğu yeniden yaratma ihtimali yok gibi görünüyor, çünkü hiçbir *şey için geniş bir Amerikalı koleksiyonu toplanamaz* . Kurumsal pazarlamacılar, kampanya yöneticileri veya sorun girişimcileri olsun bilgi uzmanları, aslında denemekten vazgeçtiler. Artık tamamen segmentasyon ve uzmanlaşma işindeler. Demokrasi için sorun, bu işin az sayıda insanı kendi önyargılarına uyan bir şeye ikna etmek için çok iyi çalışması, ancak büyük ölçekli sosyal konsensüs oluşturmaya gelince kendi kendini iptal etmesidir.

bilimsel bilgiyi bir araya getirmede bir rol oynamış olan uzman toplulukların veya *epistemik toplulukların* parçalanmasıdır . Çoğu uzmanlık alanında, sosyal medya, akademik dergilere ve diğer forumlara yayılan savaşlar aracılığıyla düzenli olarak birbirlerine saldıran köklü, rekabet eden alt gruplar var. Bazı durumlarda, vizyonlar nispeten keyfi görünüyor; hepsi ideolojik değil ve bazı alt gruplar belirli kişilikler veya akademik teoriler etrafında şekilleniyor gibi görünüyor. Giderek artan bir şekilde, akademik faaliyetin odak noktası, rakip akademik siloları itibarsızlaştırmaktır; belirli bölümler, daha önce bir düşünce okulu ile ilişkilendirildikleri gibi, şu veya bu silo ile ilişkilidir.

Küresel düzeyde paralel silolar var. Bazı otokratik devletler, parçalanmanın ortasında en azından bir miktar kalıcı cazibe ile ulusal düzeydeki anlatıları sürdürmede başarılı oldular - demokratik toplumlardan çok daha fazlası. Büyük otokrasiler, diasporaları da dahil olmak üzere ulusal veya etnik nüfuslarına eşit olan büyük yankı odaları yaratmaya ve ardından duvarları kapatmaya çalışarak bu eğilimlerden yararlanıyor. Anlatılarını ihraç etmelerinin bir yolu, yabancı şirketlere ve kuruluşlara onlarla ilişki kurma hakkı için koşullar zorlamak. Örneğin 2018'e kadar Çin, 500'den fazla akademik dergiyi, aralarında "Tiananmen", "Dalai Lama" ve "Tibet" in de bulunduğu bir avuç seçilmiş kelimeyi makalelerinden çıkarmaya zorlamıştı. 3 (Çevrimiçi sürümleri

3 Çin'in bu alandaki sansür çabaları, Evan Osnos, "Making China Great Again", *New Yorker* , 8 Ocak 2018'de anlatılıyor.

makaleler artık gizliliği kaldırılmış devlet belgeleriymiş gibi geri çekmelerle birlikte geliyor.)

Büyüyen Siber Taciz Manzarası

Eko odalarının büyümesiyle yakından ilişkili bir eğilim, trolling etiğinin patlaması olmuştur: "siloların savaşlarını" karakterize eden yaygın siber taciz. Çeşitli sosyal medya platformları, web siteleri ve hükümetlerin artan çabalarına rağmen, bilgi dünyası bu gerçeklikte özellikle daha zalim ve daha korkutucu bir yer haline geldi. ⁴

Siber taciz ve zorbalığın kökleri, kısmen, öfkeli, ironik kendi kendine yaramazlık yapan çetelerin, öfkelerini ateşleyen herhangi bir hedefe karşı büyük kampanyalar başlatmak için bir araya geldikleri sitelerde, on yıl önce ortaya çıkan devasa trolleme topluluğuna dayanmaktadır. En rezil kampanyalardan biri, oyun topluluğundaki kadınların kısır, kadın düşmanı ve bazen vahşice tehdit eden çevrimiçi saldırılara maruz kaldığı Gamergate idi. ⁵ Bu siber fırtına birlikleri toplulukları hem parçalandı hem de metastaz yaptı ve web giderek, siber saldırı dalgalarının eşit derecede kapsamlı karşılıklarla karşılandığı, herkese karşı anarşik savaşların yeri haline geldi.

On yıl önce, böyle bir saldırıyı yürütmek zahmetli bir siber ustalık eylemiydi. Her adımın elle kodlanması gerekiyordu. Bugün, bu tür saldırılar, siber araçları kullanarak insanların hayatlarını yok etmek için özel olarak oluşturulmuş yapay zeka motorları tarafından yürütülüyor. Bu *saldırı botları*, çeşitli algoritmik rehberlik kullanarak bir hedefin görünen güvenlik açıklarıyla bir başlangıç stratejisini gerçekleştirmek ve hizalamak için binlerce potansiyel eylemden oluşan bir repertuarına sahiptir. Daha sonra, hedeflere göre veya hedefler hakkında kamuya açık açıklamalar, yaptıkları eylemlerin kanıtları ve bunlarla ilgili mevcut verilerin değişen şekli gibi yanıtları izler ve devam eden kampanyayı neye göre yükseltir veya uyarlarlar.

⁴ Açık olmak gerekirse, siber taciz ve zorbalık gelecekteki olası bilgi senaryolarının önemli bileşenleri haline gelebilirdi; paylaşılan bir bilgi dünyasına içkindirler. Ancak, son derece parçalanmış ve çoğu zaman birbiriyle çatışan alt bileşenlerin olduğu bir çağda, yankı odası geleceğinin bu uygulamaların patlamasına karşı özellikle savunmasız olduğu kanıtlanmıştır.

⁵ Nagle, 2017, s. 15–17, 24–25, 35.

görüyorlar. Şimdi tek gereken siber saldırganlar veya ülkelerden birindeki bir yetkilinin bir düğmeye basması ve bir hayat fiilen yok ediliyor. Sahtecilik ve diğer gizleme yöntemlerindeki gelişmişlik nedeniyle, AI tarafından yürütülen siber saldırıların izini sürmek son derece zordur.

Bu saldırıların birçoğu, IoT'yi giderek artan bir şekilde taciz yolu olarak kullanıyor. Bir silo savaşının bir tarafında özellikle öne çıkan bir yorumcu, WiFi bağlantılı termostatin evini aşırı ısıtmak için yeniden programlandığını veya akıllı buzdolabının yüz galon süt sipariş ettiğini öğrenmek için eve gelebilir. Hedeflerin sağlığının peşinden giden, web özellikli kalp pili veya insülin pompasının ayarlarını manipüle eden ve doktor muayenehanesinde test sonuçlarını işleyen algoritmayı değiştiren daha uğursuz saldırılar oldu.

Sonuç, çevrimiçi konuşmanın ve özellikle şiddetli silo savaşlarında, yalnızca belirli içerikleri görüntülemenin bedelinin çok yüksek olabileceği bir dönemdir. Bu tür bilgi saldırganlığının tehlikesi, halk arasındaki diyalog üzerinde yaygın bir caydırıcı etkiye sahiptir.

Nihai bir yanıt olarak, hedef alınan küçük insan grupları “Off the Net” topluluklarına katılmaya başladı. Toplu olarak “Netters” olarak bilinen bu insanlar, halka açık çevrimiçi dünyadan çekilmeye karar vermişlerdi. Yenilenebilir enerji ve robotik tıp gibi en son teknolojileri kapsamlı bir şekilde kullanırken, kendilerini ağa bağlı bilgi sistemlerinden tamamen kestiler: sosyal medya, beş büyük teknoloji şirketi, akıllı evler ve internetin kendisi. 6 Yerel bankalar, hastaneler, marketler kurdular (2020'lerin başındaki Amazon Gıda Deposu devriminden bu yana görülmemiş bir yenilik), hepsi tamamen çevrimdışıydı. Etkili teşhis için gerekli olan tıbbi kayıtlar dışında dijital biçimde hiç kimse hakkında hiçbir veri toplanmaz ve bunlar üst düzey güvenlikle korunan hava boşluklu sunucularda barındırılır. Bu toplulukların birçoğu (şimdi Amerika Birleşik Devletleri'nde 8 milyondan fazla ve Avrupa'da eşit sayıda sakini içerecek şekilde büyümüşür)

6 Bu gelişmenin bir ironisi, Off the Net topluluklarının ilk başta, her elektronik sistemi bağlamak ve çalıştırmak için yüksek hızlı bir sinir sistemi bilgi boruları olmadan "aptal" bir ev inşa etmeyi bilen inşaat firmalarını yeniden bir araya getirmek zorunda kalmış olmalarıdır. Akıllı evler o kadar yaygın hale gelmişti ki çoğu inşaat şirketi başka herhangi bir şeyi nasıl inşa edeceğini unutmuştu.

kitlesel siber taciz kampanyalarının kurbanları, onlara yozlaşmış kamusal kişiliklerini geride bırakabilecekleri bir sığınak yeri sunuyor.

Bu tür saldırılarla başa çıkmadaki zorluğun bir kısmı, siber taciz uygulamasının üzerinden on yıl geçen bugün bile, kolluk kuvvetlerinin nadiren siber tacize yüksek bir öncelik vermesi veya bu konuda çok şey yapacak teknik becerilere sahip olmasıdır. Çoğu yerel polise, böyle bir saldırı, gerçek bir uzmanlığa sahip olmadıkları soyut bir vaka gibi görünecektir. Bu arada, ulusal düzeydeki kolluk kuvvetleri -bu günlerde aşırılık yanlıları, radikaller, milisler ve diğer doğrudan şiddet içeren tehditlerle boğulmuş olmanın yanı sıra- tipik olarak bir davaya dahil olmak için belirli eşiklere sahiptir. Artık ulusal düzeyde o kadar çok siber tehdit var ki, hedefler kendileri için bir siber tespit ve caydırma ajansı tutacak kaynaklara sahip olmadıkça, bireylere yönelik saldırılar genellikle araştırılmıyor.

Bu tür firmalar, teknoloji dünyasının en hızlı büyüyen bileşenlerinden biri haline geldi. Virüsten koruma yazılımı, özel dedektiflik bürosu, ev güvenlik şirketi ve mafya koruma racketinin bir kombinasyonunu temsil ediyorlar. Potansiyel müşterinin "hedeflenebilir oranına" (bir yabancı hükümetle ters düşme olasılıklarının ne kadar olduğu) bağlı önemli bir yıllık ücret karşılığında, bu firmalar siber tacize karşı bir sigorta poliçesi sunuyorlar. Olursa ve ne zaman olursa, kaynağını belirlemeye çalışacaklar; arkadaşlarınıza, ailenize ve iş arkadaşlarınıza bildirimler gönderin; saldırıda bozulan verileri düzeltin; sahte siteleri ve gönderileri kapatın; ve saldırıdan sorumlu görünen tüm ağlara karşı saldırgan eylemlerde bulunarak karşılık verin. Bazı daha sert firmalar, bilgisayar korsanlarını ziyaret etmek ve mesajı kişisel bir dokunuşla iletmek için birkaç ülkede eski özel kuvvet askerlerini bile kullanıyor.

Bu taciz modeli aynı zamanda kuruluşlara da uzanıyor. Kuzey Kore, 2014 yılında Sony Pictures'a yaptığı saldırılar ve Kuzey Kore'nin kaçırılmasıyla ilgili bir İngiliz belgeselini baltalamak için yaptığı paralel saldırıyla bu tür stratejiler için modern bir emsal oluşturdu. Kuzey Kore, filmdeki potansiyel yatırımcıları korkutmayı başardı. 7 Bu tür stratejiler günümüzde yaygın ve ABD ve Avrupa'nın önde gelen medya şirketleri

7 David E. Sanger, David D. Kirkpatrick ve Nicole Perloth, "Dünya Bir Zamanlar Kuzey Kore Siber Gücüne Gülmüştü. No More," *New York Times*, 15 Ekim 2017.

ni'ler genellikle dünyanın en büyük siber güçlerinden herhangi birini gücendireceğine inandıkları herhangi bir projeyi reddederler. Çin, Tibet de dahil olmak üzere istenmeyen konulardaki çevrimiçi tartışmaları ezmek için troller ve botlar kullandı. Bu saldırılar, belirli tartışmaları sular altında bırakmak için kullanılan hizmet reddi saldırılarının eşdeğerinin yanı sıra doğrudan tacizi de içeriyor. ⁸

Kamu ve özel aktörler arasındaki sınırların bulanıklaştığı bir dünyada, ulusal hükümetlerin doğrudan bu tür taciz kampanyaları yürütmesi gerekmiyor. Çoğu durumda, yalnızca gevşek *komut dosyasını çevirebilirler çocuklar* : agresif sosyal medya için çevrimiçi vekiller olarak hareket etmeye istekli insanlar manipülatör. İnternetteki daha büyük yankı odaları, işleri dengeleyici görüşleri denetlemek ve inanç silosuna karşı herhangi bir saldırganlığa yanıt olarak karşı saldırılar başlatmak olan “milisleri” ilişkilendirdi. Bu tür misilleme saldırıları bazen yenilikçi finansman teknikleriyle güçlendirildi. Düşman aktörler, Rus devlet kurumlarıyla, örneğin kodlayıcılara ABD hedeflerine saldırımları için ödeme yapmaları için “vatansever” Rusları (ve dünyanın dört bir yanındaki ABD gücünü azaltmak isteyen diğerlerini) kitle kaynaklı kullanarak, çabaları kitlesel olarak finanse etti. ⁹

Bu saldırgan uygulamalardaki bir diğer önde gelen eğilim, rejimlere tehdit olarak işaretlenen belirli yabancı bireyleri hedef alma çabalarıyla artan hassasiyetleri olmuştur. Bu çabaların çoğu, klasik siber zorbalık, çevrimiçi taciz ve kimlik hırsızlığı biçimini alır; bunlara, hedeflerin kişisel bilgilerini tehlikeye atmak, onların adına kredi veya kredi kartı almak ve ev ve iş e-posta hesaplarına tehdit mesajları göndermek dahildir. Ancak bazı kampanyalar, siber tacizin diğer birçok biçimine yönelik bu sıradan yaklaşımların çok ötesine geçti: iddiaya göre bilgi sızdırdığı iddia edilen yanlış web siteleri oluşturmak; Hedefleri çalma, öldürme veya samimi bağlamlarda gösterdiği iddia edilen yüksek kaliteli dijital taklit programları kullanarak sahte videolar oluşturmak; hedeflerin vergi veya polis kayıtlarını bozmak için resmi veri tabanlarını hacklemek; düzinelerce arkadaş ve meslektaşına kritik e-postalar göndermek; ve hedefleri hacklemek'

8—Segal, 2016, s. 215.

9 Bu strateji zaten kanıtlanmıştır; bkz. Hannes Grassegger ve Mikael Krogerus, “Weaken from Within,” *New Republic* , 2 Kasım 2017.

sosyal medya sayfalarında sözde kendi adlarına saldırgan materyal yayınlamak. ¹⁰ Saldırıları ayrıca, bir hedefin dairesine uyuşturucu yerleştirmek ve ardından polise haber vermek veya kuryelerin görünüşte elle yazılmış notları teslim etmesini sağlamak gibi gerçek dünyadaki eylemleri siber saldırılarla birleştiriyor. Ama her şey uzaktan yapılır. Mesajların kökenini gizlemek için sahtecilik tekniklerini kullanarak, görünüşte hedeften *kaba* ve kendi kendini suçlayan e-postalar bile gönderirler .

Bilgiye Dayalı Saldırganlık ve Silo Geleceği

Baskın yankı odalarının daha parçalı bir bilgi-küresinin ortaya çıkması, bilgi temelli saldırganlık için muazzam bir nimet olduğunu kanıtladı.

Açık bir teknik, özellikle aşırı, şikayet kaynaklı ve paranoyak inanç silolarını belirlemek ve üyeleri şiddetli sosyal hoşnutsuzluk seviyelerine çıkarmak olmuştur. Halihazırda, bazıları şiddete dönüşen, bu gruplara pompalanan uydurma (veya abartılı) bilgilerle teşvik edilen birçok yerel protesto örneği var. Bu saldırılar aynı zamanda, bazı durumlarda doğrudan sosyal medya platformlarından veya pazarlama firmalarından alınan veya düzinelerce belirli veri hırsızlığından özenle oluşturulmuş, yabancı güçler tarafından Amerikalılar hakkında bireyselleştirilmiş verilerin devasa veritabanlarının edinilmesiyle de körüklendi. Moskova'da ABD'deki herhangi bir siyaset bilimcisinin daha kesin olarak ayarlanmış bir ABD sosyal dinamikleri anlayışına sahip bir grup sosyal bilimci olduğu söyleniyor, ancak bu sadece bir söylenti.

Bu süreçte, bilgi saldırganları, büyük gruplardaki doğal sürü davranışlarından yararlanıyor; bu, nüfusun geneline kıyasla yankı odaları arasında daha da tutarlı. Manipülatörler, belirli bir sosyal ağlarda bir siloya veya yankı odasına hükmeden ve ardışık tartışmaları tetikleyen etkileyicileri ustalıklı hedef alır.

¹⁰ Bu örneklerin çoğu, Brooke Jarvis'in "Me Living Was How I was How I Was How I Beat Him Beat Him," *Wired* , Aralık 2017'de açıklanan vakadan alınmıştır. 2016 yılına kadar 10 milyondan fazla Amerikalı'nın tehdit edildiğini bildirdiği bir istatistikten alıntı yapıyor. , ya da müstehcen görüntülerin çevrimiçi olarak yetkisiz paylaşımına maruz kaldı.

ve inanç - ve eğer şanslılarsa, öfke ve küskünlük - bazen uydurma, bazen sadece abartılı hikayelere dayanır.

Bu süreçte, bilgi saldırganları da karşılıklı şüpheleri yoğunlaştıran hikayeler (bazen gerçek, bazen değil) yayarak ABD toplumunun silolaşmasını şiddetlendirmeye çalışıyorlar. Liberal bilimsel temalar etrafındaki yankı odaları, dengeleyici siloları yöneten muhafazakar bilim adamlarının kötülükleri hakkında düzenli bir bilgi akışı elde edecek ve popülist yankı odaları, günlük olayların komplocu “derin durumu” eylemde nasıl yansıttığı hakkında bilgi bombardımanına tutulacak; bir düzine alternatif yankı odasından biri adına konuşan hiç kimseye güvenilmemelidir. Bu eğilimler bilgi dünyasında oldukça ilerlemekteydi ve manipülatörlerin birlikte çalışması için mükemmel hammadde sağladılar.

Toplumsal saldırganlık kampanyaları, bilgi ortamının giderek artan şekilde yapay zeka güdümlü, otomatikleştirilmiş yönlerini demokrasilerin aleyhine çevirmektedir. Şu anda düşman güçler ve gruplar tarafından kullanılan önemli bir araç, hedeflenen pazarlamacıların bilgi balonlarına erişmek için kullandıkları algoritmaların bozulmasıdır.¹¹ Bazı durumlarda, öfke ve düşmanlığa neden olmak için çok taraflı, düşmanca mesajları spektrumun karşı tarafına yönlendirirler. Ya saldırganın bakış açısına uygun olan ya da sadece endişeye neden olan belirli hikaye dizilerini insanlara iletmek için gazete algoritmalarını hackleyecekler.

Bu gelecek hızla ve sosyal ve demokratik istikrara açıkça zarar veren şekillerde geliyor. ABD halkının (ve diğer ileri demokrasilerin halklarının) silolaşma derecesi karışıktır; bazıları diğerlerinden çok daha özel yankı odalarına gömülüdür ve paylaşılan algılar üzerindeki etki tek tip değildir. Ancak genel eğilim, bu gelişmelerin hızlanması ve derinleşmesi ve özellikle silolar arasında artan düşmanlığın ve doğrudan bilgi çatışmasının yükselişi olmuştur. Nereye gittiği ve karşı trendlerin yakında ortaya çıkıp çıkmayacağı belirsizliğini koruyor.

11 Danah Boyd, “Your Data Is Manipulated,” *Data and Society, Points*, 4 Ekim 2017.

Gelecek 3: Algoritmaların Yükselişi (2026 Senaryosu)

Genel Gelecek

2026'ya kadar olan on yılda, herkes hakkında çok miktarda kişiselleştirilmiş bilgi, IoT, sosyal medya, tıp, hukuk, istihdam ve bir düzine başka alanda büyük veritabanlarına entegre edildi. Hem kamu hem de özel kuruluşlar giderek artan bir şekilde bu bilgi selini anlamlandırmak için algoritmik karar verme yöntemini kullanıyor. Süreç, internet arama sonuçlarını belirlemek ve tüketicilere tarama ve satın alma geçmişlerine dayalı önerilerde bulunmak için algoritmalar ile başladı - “bunu beğendiyseniz, buna bayılacaksınız” modeli. Ama şimdi algoritmik karar vermenin kullanımı bir düzine farklı alana yayıldı. Günümüzde algoritmalar, hastalıkların tedavisi (ve devam eden tedavinin artık haklı görülmediği nokta), suçluların cezalandırılması, çalışanların işe alınması, şehirler arasında kolluk kuvvetlerinin konuşlandırılması hakkında karar verir veya en azından kararlar için güçlü ilk tavsiyelerde bulunur. , ve daha fazlası. Bu algoritmalar, algoritmik bir çağın temel temeli üzerine kuruludur: vatandaşlar üzerinde mevcut olan veri okyanusları veya *bilme bulutu olarak adlandırılabilir şey* .

Algoritmik karar verme birçok yönden insan yaşamını iyileştirdi. Bir dizi hastalık ve tıbbi durumla ilgili olarak benzeri görülmemiş bir tahmin doğruluğu sunarak, bazı durumlarda hızlı tedavi ve iyileştirmelere izin verdi. Suç oranları üzerinde ölçülebilir etkileri olan bazı şehirlerde hedefli polisliği güçlendirdi. Bazı özel durumlarda, cezalandırmaya yeni bir objektiflik derecesi getirerek, bazı yeni suçluların karşı karşıya kaldıkları cezaları

belirli suç kategorileri ve bu alanlarda genel olarak gelişmiş adalet olarak görülen şeyleri üretmek. Karbon emisyonlarını azaltma hedefine katkıda bulunan, enerji kullanımları da dahil olmak üzere binlerce işletmenin verimliliğini ölçülebilir şekilde iyileştirdi.

Ancak bu tür algoritmaları dağıtma acelesi, sosyal etkileri hakkında fazla bir gözetim veya tartışma olmaksızın parça parça gerçekleşti. Ve olumlu potansiyellerine rağmen, sosyal manipülasyona karşı savunmasızdılar ve iyi anlaşılmayan karmaşık sonuçları olan makine güdümlü karar verme yönünde daha büyük bir eğilimin göstergesidirler.

Bilme Bulutu

Son birkaç yılda, büyük veri, nesnelerin interneti, yapay zeka ve daha fazlası gibi bilgiyle ilgili birkaç teknolojideki ilerleme hızlandı ve ortaya çıkan tek bir gerçeklik etrafında birleşti: her biri hakkında büyük miktarda verinin yoğun, paylaşılan farkındalığı. gelişmiş dünyadaki bireysel insan (ve aynı zamanda gelişmekte olan dünya popülasyonlarının daha küresel olarak bütünleşmiş unsurları). Bu sistemlerdeki toplam veri miktarı, her iki yılda bir kabaca ikiye katlanmaya devam etti; ¹, devasa yeni bulut tabanlı veri barındırma hizmetleri, yapay zeka güdümlü arama ve işleme işlevleri ve diğer barındırma ve barındırma araçları için gereksinimler (ve pazarlar) oluşturuyor. Bu akıllara durgunluk veren miktarda bilgiyi manipüle etmek.

Yıllardır her insan seçimler, tercihler, alışkanlıklar, kişisel bilgiler, ilişkiler, satın almalar ve çok daha fazlasını içeren bir "dijital egzoz" ² bırakıyor. On yıl veya daha uzun bir süredir, herkesin çevrimiçi olarak yaptığı her hareket, büyük ölçüde çeşitli siteler tarafından kullanıcının tarayıcısına gönderilen izleme “çerezleri” kullanılarak izlendi, kataloglandı ve değerlendirildi. insan

1 Uluslararası Veri İşbirliği, “Yönetici Özeti: Veri Büyümesi, İş Fırsatları ve BT Zorunlulukları”, *Dijital Fırsat Evreninde: Zengin Veri ve Nesnelerin İnternetinin Artan Değeri*, Framingham, Mass., Nisan 2014.

2 Terim, Dale Neef, *Digital Exhaust*, Upper Saddle River, NJ: Pearson FT Press, 2014'ten gelmektedir. Ayrıca bkz. National Public Radio, “Big Data Revolution,” *TED Radio Hour*, 9 Eylül 2016.

ple'in film seçimleri, web aramaları, çevrimiçi sözlüklere girdileri, tweet'leri ve sosyal medya yorumları olağanüstü miktarda veri üretti. 2016 yılına kadar Acxiom, Cambridge Analytica ve benzeri firmalar her Amerikalı hakkında 1.000 ila 5.000 bireysel bilgi topladı. 3 IoT'nin ortaya çıkmasıyla birlikte bu akış patladı ve giderek birbiriyle bağlantılı hale geldi. Milyarlarca cihaz artık paylaşılan veri sistemlerine bağlı ve giderek küçülüyor, birçok akıllı sensör artık insan gözünün görebileceğinden daha küçük. Bazı tahminler, mevcut 500 milyar IoT cihazının halihazırda dünya gayri safi yurtiçi hasılasında (GSYİH) yaklaşık 3 trilyon doları oluşturduğunu gösteriyor. 4

Her yerde bulunan algılama ve veri toplama, akıllı buzdolabı tarafından algılandığı gibi, insanların sütlerini ne kadar hızlı içtiği de dahil olmak üzere artık milyonlarca farklı konuda bilgi topluyor; akıllı tuvaletleri tarafından değerlendirilen kişisel atıklarının kalitesi; çocukken söyledikleri, akıllı oyuncaklarıyla kaydedildiği ve arşivlendiği; 5 iPad'lerindeki haber aboneliklerinin bildirdiğine göre, erkek İngiliz film yıldızlarının aksine ABD'li kadın romancılar hakkındaki hikayelerde ne kadar süre oyalanıyorlar; vücutlarının kesin ölçümleri ve sanal moda asistanlarının kendileri için doğru gardırop seçmelerine yardımcı olan yüzlerce veri noktası (kişilikle ilgili birçok); 6 ve sosyal medya gönderilerinde ifade ettikleri fikirler, AI güdümlü botlar tarafından izlenir, derlenir ve analiz edilir. Her gün, bu tür terabaytlarca veri, tıbbi, psikolojik ve eğitim geçmişlerinin en ince ayrıntıları da dahil olmak üzere, kamuya açık ve kolayca hacklenebilir veritabanlarında mevcut olan kişisel bilgilerin hazinelerine katılıyor ve bunların tümü, sağlığı hedefleyen makine öğrenimi analitiğine izin vermek için bir arada depolanıyor. , günlük ruh halleri ve konumları (ve kalıcı konum geçmişi) ile yeni FitBit ifadeleri veya diğer mobil fitness izlemeleri tarafından izlenir

3 Pariser, 2011, s. 6-7.

4 Yazılımın ve Toplumun Geleceği Küresel Gündem Konseyi, 2015, s. 8.

5 Erik Silfversten, "Akıllı Bir Oyuncak Sadece Noel İçin Değil, Yaşam İçin Kişisel Ayrıntılara Sahip Olabilir," *RAND Blog* , Aralık 2017; Norveç Tüketici Konseyi, *#Toyfail: Bir Analiz İnternet Bağlantılı Üç Oyuncakta Tüketici ve Gizlilik Sorunları* , Oslo, Aralık 2016.

6 Drew Harwell, "Şirketler Yeni Ödül Kazanan Bir Para Birimi: Vücut Ölçümlerimiz", *Washington Post* , 16 Ocak 2018.

cihaz. 2021 yılına kadar, her yıl yaklaşık 250 milyon bu tür giyilebilir cihaz satılıyordu. ⁷

Bulut (insanlar artık yaşamları boyunca asılı kalan ve her seçenek ve fırsata yığılan veri yığınının kısa bir tanımı olarak kullanıyorlar) çocuklarınızın dikkat eksikliği/hiperaktivite bozukluğu (DEHB) tedavisi görüp görmediğini, hangi ilaçları aldıklarını bilir. en son notlar ve ikisi arasındaki ilişki (ve her birinin diğer bin değişkenle ilişkisi). Öğretmenlerinin onlar hakkında ne düşündüklerini ebeveynlerinin bildiklerinden çok daha fazla bilir. Arkadaşlarınızın kim olduğunu bilir, alışkanlıklarını ve tercihlerini bilir ve bu verileri iyi bir istatistiksel olasılığa kadar davranışınızı tahmin etmek için nasıl kullanacağını bilir. Yazarken kullandığınız dili (favori kelimeler ve ifadeler, yaygın gramer hataları vb.) ve bunun kişiliğiniz ve tercihleriniz hakkında ne söylediğini bilir. GPS özellikli sensörler (artık esas olarak Amerika Birleşik Devletleri'nde satılan her yeni araçta standarttır) tarafından toplandığı ve otomobil şirketi aracılığıyla iletildiği şekilde arabanızı nereye sürdüğünüzü bilir ve sonuç olarak davranışınız hakkında güçlü çıkarımlar yapabilir. . ⁸ (İçki dükkanına yapılan düzenli geziler sisteme bir şey söyler; acil bir bakım merkezindeki ani duraklamalar sisteme başka bir şey söyler.) Sürekli gözetim ve yüz tanıma sayesinde, hangi ruh halinde olduğunuzu bilir ve bazı durumlarda , düşündüğünüzü tahmin edebilir.

Gerçekte, giderek artan bir şekilde, toplumdaki finansal, sosyal veya politik her öge, topladığı ve ilettiği verilerden çok, ne olduğu için daha az önemlidir. Otomobiller artık orijinal uzay mekine göre 200 ila 300 kat daha fazla kod satırına sahip. ⁹ Bir çocuk oyuncağı, eski süper bilgisayarların işlem gücüne sahiptir. Bebekler, iPad'ler, egzersiz ekipmanları, diyabetik sensörler ve çok daha fazlası, The Cloud'a ve bundan faydalanmak isteyenlere kullanıcıları hakkında söyledikleri için çok değerlidir. Şirketler fiziksel ürünleri kayıp liderleri olarak satıyorlar

⁷ Patrick Tucker, "Strava's Just Start: ABD Ordusu Veri Sızıntısına Karşı Savaşı Kaybediyor," *Defense One* , 31 Ocak 2018.

⁸ Peter Holley, "Gezicilerdeki Büyük Birader: Neden Araba Şirketiniz Sizin Hakkınızda Eşinizden Daha Çok Şey Biliyor olabilir," *Washington Post* , 15 Ocak 2018.

⁹ 2018'deki sayı 200 kat daha fazlaydı (Holley, 2018).

müşterileri kalıcı bir bilgi ilişkisine sokmak. Ve çeşitli bilgi ağları üzerinden inanılmaz derecede büyük sellerde akan bu bilgi, genellikle zayıf bir şekilde korunur ve akan veri akışlarına bir araştırma tavası sokmaya istekli hemen hemen her girişimci hacker tarafından kullanılabilir.

Yaklaşık 2020 boyunca, bu eğilimler mahremiyet hakkında bir tartışma yaratmaya devam etti. Bu terim artık büyük ölçüde kamusal diyalogdan çıkarılmıştır. Uzak bölgelerde yüksek teknoloji ancak “verisiz” topluluklar oluşturan küçük ama artan sayıdaki “Off the Netters” dışında, geçerli varsayım, yaptığınız, söylediğiniz, inandığınız veya satın aldığınız (eğer öyleyse) her şeyin olduğudur. bizi çevreleyen sensörler ve bot dizisinden bilinçli olarak gizlenmemiş) şimdi Bulut'a yakalanıyor. Amaç artık bu gerçeklikle savaşmak değil, onun içinde gezinmek ve onu mümkün olan en iyi şekilde kullanmaktır.

Artık Buluttan kopuk “özel benlik” diye bir şey yok. Yalnızca kolektif bir benlik, gerçek benliklerimizin sanal bir temsili olarak var olan ve her gün bir milyon AI tarafından yazılan eylemi yöneten devasa bir veri koleksiyonu vardır. ¹⁰ Ve bu koleksiyon gitgide devasa ve birbirine bağlı bir algoritma örümcek ağı tarafından düzenleniyor.

Gerçek, kısmen yükselen çağın temel teknoloji şirketlerinin devam eden büyük büyüme eğilimi nedeniyle kaçınılmaz hale geldi: Alphabet (Google), Apple, Facebook, Amazon ve Microsoft. ¹¹ Büyümeleri, hızlanan bir kâr döngüsü, yenilikçi firmaları ele geçirme, yeni yetenekler yaratmak için araştırma ve geliştirme ve artan pazar payı (ve dolayısıyla daha fazla kar) tarafından desteklendi. Tıbbi veriler, içerik sağlama veya akıllı ev ağları gibi anlamlı herhangi bir alanda onlara meydan okumaya çalışan herhangi bir yeni firma veya firma grubu ezildi veya satın alındı. Yüksek teknoloji çağından beklenenin tersi oldular: küçükten çok büyük,

¹⁰ Veri analizi yapabilen sinir ağlarının büyümesi hakkında bkz. Cade Metz, “Final, Neural Networks That Really Work,” *Wired*, 21 Nisan 2015.

¹¹ Çin'in paralel bir dizi firması var - AliBaba, Baidu, Tencent ve diğerleri - ama büyük ölçüde dış internetten duvarlarla çevrilmiş durumdadır. Çin'in ötesindeki erişimleri, ana anakara ağlarından hava boşluklu olan ve Asya'daki etnik Çin diasporasına hizmet eden ikincil ağlarla sınırlıdır.

taban otoritesi yerine merkezi kontrol. En son tahmin, bu beş şirketin birbirine bağlı büyük veri dünyasının veritabanları, şirketler ve teknolojiler gibi tüm unsurlarının yüzde 85'i gibi bir şeyi kontrol ettiği yönünde.

Etkileşimli Veri

Yaklaşık 2019-2020 boyunca, bu veriler, pazarlamacılar veya politikacılar tarafından satın alınabilecek veya web siteleri tarafından satışları artırmak için kullanılabilir, büyük ölçüde soruna özel bir olgu koleksiyonu olarak kaldı. Amazon, insanların satın aldıklarını ve baktıklarını gelecekteki ilgiyi tahmin etmek ve satışları artırmak için kullandı, Google, hedefli pazarlama için arama motoru algoritmalarını mükemmelleştirmeye devam etti ve bir ilaç şirketi, ürününü satmak için insanların tıbbi geçmişlerine ilişkin verileri satın alabiliyordu. Ancak son iki yılda, AI yeteneklerindeki ve teknoloji şirketi birleşmelerindeki bir artışın tetiklediği Bulut, birbirine çok daha bağlı ve çok daha akıllı hale geldi. Şimdi, en azından algoritmik tahmine en çok tabi olan belirli bir bireysel ve toplu eylemler kategorisi hakkında şaşırtıcı bir doğrulukla tahmin ediyor, değerlendiriyor ve tahmin ediyor.

Birkaç tuş vuruşuyla, Bulut öğelerini denetleyen veri mühendislerinden biri (ancak makine öğrenimi güdümlü yapay zekanın patlamasıyla, "gözetim" fikri giderek daha az anlamlı hale geliyor) birçok şey hakkında son derece doğru bir izlenim edinebilir. herhangi bir birey hakkında: nerede oldukları ve nereye gitmeyi planladıkları - ve nereye gitmeleri muhtemel; ne satın aldılar; ve yüzde 70-80 olasılıkla gelecek ay ne *alacaklarını* . Bu bilginin kökenleri, uzun süredir birinin belirli bir filmi ne kadar iyi seveceğini tahmin edebilen Netflix gibi firmalar tarafından geliştirilen algoritmalarda yatar ve kabaca yüzde 10'luk bir hata payıyla.¹²

Aynı zamanda, Bulut artık bu tür analizleri üstlenmek veya bu tür seçimler yapmak için bilinçli insan müdahalesini beklemiyor. İnsan davranışını artan doğrulukla öngören, çoğu durumda uygulanan ve sürekli olarak verileri değerlendiren bir milyardan fazla AI güdümlü bot tarafından sürekli olarak rafine edilen milyonlarca amaca yönelik algoritmaya ev sahipliği yapmaktadır.

¹² Pariser, 2011, s. 8.

ve daha sonra önceden programlanmış hedefleri ilerletmek için harekete geçin. Geniş bir şekilde birleştirilmiş bir bulutun IoT ve diğer ağa bağlı yönleriyle, mesajlar, reklamlar, izleme işlevleri ve bu sürecin diğer iletişim noktaları, kullanıcıları cihazdan cihaza, siteden siteye ve yerden yere takip eder. Bulut, müdahalede bulunmadan eylemleri gözlemler ve bunlara yanıt verir. Birçok önemli açıdan sürücüsüz bir ağıdır. Pariser 2011'de "Reklamlarımızı yöneten algoritmalar hayatımızı düzenlemeye başlıyor" diye yazmıştı. ¹³ Bugün, 2026'da bu etki her yerde görülüyor.

Ve Bulut giderek gerçek zamanlı olarak çalışır. Birinin dijital egzozunun, haftalar hatta aylar sürebilen veritabanlarında zahmetli bir şekilde toplandığı günler geride kaldı. Artık insanlar bir düzine anlık bilgi toplama sensörüyle etkileşime giriyor: saatler, implantlar, yerleşik kameralar ve mikrofonlar, sosyal medya platformları ve daha fazlası. ¹⁴ Radyo frekansı tanımlama (RFID) cihazları, satın aldığımız hemen hemen tüm anlamlı ürünlere yerleştirilmiştir ve bu, şu anda ülke genelinde milyarlarcası bulunan herhangi bir RFID sensörünün menzilinden geçtiklerinde izlenmelerini sağlar. Eşyalarınız bile dijital *egzoz* üretiyor. ¹⁵ Sonuç, mesajlar (reklamlar gibi) üreten ve daha sonra bu mesajlara verilen tepkilere göre yinelenen, sürekli güncellenen bir davranış ve tercih duygusudur.

Sonuç olarak, etkileşimli platformlar ve sistemler çok daha duyarlı ve çevik hale gelmek zorunda kaldı. 2019 yılına gelindiğinde, mağazalara, yürüdükleri belirli kişilere belirli ürünler ve indirimler sunan, bazen AR kulaklıklarında yayınlanan (ya da AR karikatürleri olarak üretilen) video afişleri ve hoparlörlerden oluşan temel kişiselleştirilmiş reklam sistemleri geldi. akıllı telefonları tarafından çekilen görüntüler). Ancak ilk başta, bunlar tek, esnek olmayan mesajlardı. 18 ay içinde bu, çevik, duyarlı bir etkileşime yol açtı: Sistem bir reklam yayınlıyacak, duygusal ve biyofiziksel tepkiyi ölçecek, bakalım mı?

¹³ Pariser, 2011, s. 9.

¹⁴ 2021 yılına gelindiğinde Amerikalıların üçte biri, sağlık verilerini tıp uzmanlarına iletmek için tasarlanmış küçük implantları önkollarına kabul etmişti, ancak bu aynı zamanda pazarlamacılar reklamlara ve ürünlere yönelik duygusal tepkilerin saniye saniye okumalarını da sunuyordu.

¹⁵ Pariser, 2011, s. 198.

kişi bakmak veya düşünmek için yavaşladı ve ardından mesajı uyarladı. ¹⁶ Fiyatı düşürebilir, bu birey üzerinde etkili olduğuna karar verilen (davranışsal ekonomi içgörülerine dayanan) bir dizi "dürtme"den birine girebilir, ünlü bir kişinin sanal avatarından bir mesaj sunabilir veya daha fazlasını yapabilir. Bulut, dünyanın insanlarla sürekli olarak son derece kişiselleştirilmiş bir şekilde etkileşim kurmasını sağlamıştı.

Bununla birlikte, sorunun bir kısmı - önemi çok az kişi tarafından önceden tahmin edilmiştir - algoritma tasarımcılarının bile çoğu zaman yaptıkları sonuçları neden tükürdüklerini tam olarak bilmemeleridir. Bu başlangıçta yeterince açıktı: Gezegendeki en karmaşık arama algoritmalarından bazılarının yazarları olan Google kodlayıcıları denklemi oluşturup verilerin gelmesini izleyebilirdi, ancak belirli bir noktada işin içinde çok fazla değişken vardı. çıktılara olan nedensel bağlantıları artık takip edemeyeceklerini söyledi. Algoritmik makinelerinin neden yaptıkları sonuçları ürettiğini açıklayamadılar. Bu gizem, örneğin bir internet aramasının kesin sonuçlarını açıklayamadıklarında daha az önemliydi. 2026'da, sağlık hizmeti kararlarından ipotek onaylarına ve cezai hükümlere kadar her konuda kesin sosyal seçimler üreten algoritmalarla birlikte, insanlar standart sorunun "sayılar yalan söylemez" yanıtına itiraz etmeye başlıyor. Açıkçası yalan söyleyip söylemediklerini kimse bilmiyor. Herkesin bildiği tek şey, algoritmaların çalıştığını kanıtlayan üst düzey ilişkisel kalıplardır. Ancak, ilaç yerine kalp ameliyatını veya beş yerine on yıllık bir cezayı öneren bir çıktı gibi belirli bir vakanın aykırı değer olup olmadığını kimse kesin olarak bilemez.

Şaşırtıcı bir veri kaynağı, son on yılda sohbet robotlarının patlamasından geldi. Yaygın kullanım ve tepki alan ilk kişilerden biri, etkileşimli makine öğreniminin riskleri konusunda güçlü bir uyarı görevi gören Microsoft'un Tay'ı oldu. Troller sistemi bozmaya karar verdi ve Nazi sempatizanlarının sesiyle yorumlarla doldurdu ve etkileşimlerinden "öğrenen" Tay, bu yorumları pek çok şüphelenmeyen kullanıcıya tekrar etmeye başladı. Müteakip çabalar çok daha güvenilir ve gerçekçi hale geldi: Bunu bir Çin versiyonu (Xiaoice, ayrıca Microsoft'tan) hızla izledi ve 2016'ya kadar

¹⁶ Silhavy ve diğerleri, 2017, s. 377.

Bazı kullanıcıların bota olan sevgilerini ilan etmelerini isteyen, oldukça iyi karşılanan diyaloglar. ¹⁷ İnsanlar ve sohbet robotları arasında güçlü bağ dokusu oluşturmak, birçok kişinin tahmin ettiğinden daha kolaydı.

Facebook'ta son iki yılda, kişiye özel telefon uygulamaları veya sadece çevrimiçi olarak, sohbet robotları, on yıl önceki uygulama çılgınlığının 2020'lerdeki karşılığı haline geldi. Her biri biraz farklı bir odak noktasına sahip olan ve tümü değişen gelişmişlikteki AI motorlarına dayanan binlerce kişi ortaya çıktı. Birçoğu, klinik psikologların bilgeliği ordularıyla programlanmış danışmanlardır. Bazıları eğitmendir: EVM özellikli telefonunuzu sizi basketbol oynarken (veya egzersiz yaparken veya bisiklete binerken) izleyecek şekilde ayarlayın ve ardından videoları eğilimler ve sorunlar açısından değerlendiren AI koçunuzla sonuçları tartışın. Bazıları dini danışmanlar veya yaşam koçlarıdır. Bazıları eğitici ve binlerce konunun herhangi birinde uzman olarak hareket eder. Bazıları sadece arkadaşdır, herhangi bir ırk, cinsiyet, etnik köken, din, kişilik, yaş veya isteyebileceğiniz diğer herhangi bir varyasyonda mevcuttur. (Buna yatkın olanlar için çok çeşitli yapay romantik partnerler vardır.) Bazıları tarihi şahsiyetler, diğerleri ise günümüzün ünlülerinin, sporcularının veya politikacılarının avatarlarıdır.

Sohbet robotlarının ilk sürümleri kesinlikle metinseldi: bir mesaj girin, AI odaklı bir yanıt alın. Genellikle, birinci nesil yapay zeka motorlarının hayalini kurduğu bazı aptalca tepkilere gülmek için sadece bir şaka için iyiydiler. Bununla birlikte, çok hızlı bir şekilde, yinelenen iyileştirme ve makine öğrenimi sayesinde, geliştiriciler avatarlar ve ardından AI motorunun dikte ettiği yanıtları "söyleyen" insan formlarının son derece gerçekçi düzenlemelerini oluşturdular. Şimdi, birkaç eski metin, birçok sesli ve artan sayıda yüksek kaliteli video sürümleri de dahil olmak üzere çok çeşitli sohbet robotları var; bunlar o kadar gerçekçi ki, Skype veya başka bir çevrimiçi portal aracılığıyla karşılaşıldığında çoğu kullanıcı basitçe reddediyor. gerçek bir insanla etkileşime girmediğine inanmak.

¹⁷ Bkz. Hannah Devlin, "İnsan-Robot Etkileşimleri 'Duygusal' Sohbet Robotu İle Adım Atıyor," *The Guardian* , 5 Mayıs 2017; Liz Tracy, "Tay'in aksine, Microsoft'un Çinli Chatbot'u Xiaolce, Aslında Hoş", *Ters* , 26 Mart 2016; ve Taylor Soper, "Çin'deki İnsanlar Microsoft'un Xiaoice Sanal Arkadaşını Neden Seviyor ve Yapay Zeka Hakkında Ne Diyor," *GeekWire* , 25 Kasım 2015.

Bulut Nerede Olduğunuzu ve Ne Düşündüğünü Biliyor

Yoğun kullanıcı anlaşmaları açıkça belirtse de, kullanıcıların genellikle fark etmedikleri şey, bir sohbet robotuyla etkileşim kurarken söyledikleri veya yaptıkları her şeyin kaydedildiği, işlendiği ve IoT'nin diğer unsurları tarafından kullanılmak üzere değerlendirildiğidir. Bulut. Görüşleri, düşünceleri, chatbot tarafından ortaya atılan fikirlere tepkileri, hazırlıksız yorumlar ve hatta botla konuşurken neler yapabilecekleri (karalama, örgü, telefonla çoklu görev vb.) kaydedilir. Sohbet robotlarında “etkileşim zamanı” satmak artık çok büyük bir pazar. Bir şirket, kullandığınız bir yemek pişirme eğitimi botunda 30 saniye satın alabilir, onu size belirli bir ürün önermesi için yönlendirebilir, tepkinizi algılayabilir, değiştirip yineleyebilir ve ardından satın alıp almadığınızı görmek için sonraki satın alımlarınızı takip edebilir.

Bazı yerlerde Bulut, bazılarının “dijital geçmiş” olarak adlandırdığı son olayların devam eden bir kaydını içeriyor. Kapalı devre televizyon (CCTV) kameraları, Bulut'a bağlanmayı kabul eden özel güvenlik kameraları ve sürekli dönen dronlardan oluşan bir ağ, belirli bir şehrin devam eden bir video portresini sürdürür ve bir tür kalıcı gözetim oluşturur. . Bir suç meydana geldiğinde, polis o an için dijital kayıtlara geri dönebilir ve daha sonra geriye doğru çalışarak suçluların suçtan önceki rotasını keşfedebilir veya ileriye doğru hareket ederek hareketlerini izleyebilir. Kısmen kanun ve düzen odaklı varlıklı hayırseverlerin cömert bağışlarıyla finanse edilen ülke genelindeki 18 kolluk kuvvetleri, tutukladıkları herkesin fotoğraflarından oluşan ve yaygın yüz tanıma (PFR) ile birlikte kullanılabilecek ortak bir fotoğraf veritabanı oluşturuyor.) şüphelileri bulmak için. 19

Bu geriye bakma yeteneği, PFR sistemleri biçimindeki gerçek zamanlı gözetime bağlandı. Günümüzde çoğu kentsel alanda, algılamadan kasıtlı olarak kaçmayan insanlar, yüksek çözünürlüklü yüz tanıma teknolojileri tarafından sürekli olarak taranacaktır.

18 Böyle bir sistem Irak'taki isyancıları izlemek için zaten kullanılmış ve Ohio, Dayton'da deneme amaçlı olarak konuşlandırılmıştır. Bkz. "Gökyüzündeki Göz", *Radiolab* , 18 Haziran 2015.

19 Parisier, 2011, s. 194-195.

bir saniyeden daha az maruz kalma süresiyle yüzde 90'ın üzerinde doğruluk. Tarayıcılar, şüpheli kişilere dijital "ayak bileği bilezikleri" atayabilir ve sistem, hareketlerini sürekli olarak izleyecektir. ²⁰ Çoğu büyük şehirde polis, şimdi, şüpheli suçluları arayan, geçen vatandaşları sürekli yüz tanıma araması yapan kameralı güneş gözlükleriyle donatıldı. ²¹ Sistem aranan bir kişiye çarptığında, polis gelene kadar bireyi alıkoymak için bölgeye koşan izci dronlara otomatik sinyaller gönderilir. Bazı şehirlerde, jaywalkerların bir kavşağa yaklaştığını algıladıklarında, telefonları yazılı bir uyarı ile bip sesi çıkarır; büyük miktarda tuvalet kağıdı veya kağıt havlu alan umumi banyoları kullanan kişiler de benzer bir not alır.

Bu geniş tabanlı gözetim sistemlerine, kameralar tarafından yakalanan sahnelerdeki en küçük ayrıntıları algılayabilen EVM teknolojileri de katılmıştır. Bu ayrıntılar, bir kişinin göz kaslarının seğirmesinden, deriden algılanan damarlardaki kan akışındaki değişikliklere ve katı nesnelerdeki en küçük kaymalara kadar her şeyi içerebilir. ²² Güneş gözlüğü, şapka ve sakal gibi dikkat dağıtıcı unsurlarla tanıma sisteminden kaçmaya çalışan kişiler, kimlik kontrolleri için rutin olarak durdurulur. Böyle sürekli bir gözetimin olduğu yerde, hiç kimse algılanmadan hareket edebileceğinden emin olamaz. Ancak gözetleme genellikle yardımcı olarak faturalandırılır: iPad'lerimiz ve Kindle okuyucularımız artık okuduğumuz her kitaptaki her fikre tepkimizi algılıyor. ²³

²⁰ Çinli firma SenseTime tarafından 2018 itibarıyla geliştirilen teknolojilerin bir açıklaması için bkz. Osnos, 2018. Aşağıdaki karşıdan karşıya geçme ve tuvalet kağıdı örnekleri bu hesaptan alınmıştır.

²¹ Zheping Huang, "Çin Polisi Yüzleri Tanıyabilen Güneş Gözlüğü Takıyor," *Savunma Bir*, 9 Şubat 2018.

²² Wu ve diğerleri, 2012.

²³ Yuval Noah Harari, "Big Data, Google and the End of Free Will," *Financial Times*, 26 Ağustos 2016'da önerilmiştir.

Algoritma Tarafından Yönetilen: Papa'ya Teslim Olmak

Sistemin Orwellvari sonuçları, düzinelerce yardımcı ve hatta hayat kurtaran uygulama raporlarıyla yumuşatıldı. Kayıp çocuklar dakikalar içinde kurtarıldı. Kaçırılan çocuklar kurtarıldı: Ebeveynler çocuklarına bir menzil uyarısı koyabilir, böylece sistem onların evden veya okuldan aile tarafından önceden ayarlanmadan bir milden fazla uzaklaştıklarını tespit ederse, polis gönderilir. İntiharlar önlendi. EVM kameraları ve AI motorları tarafından yaklaşımakta olan felçler teşhis edildi ve inme meydana gelmeden hemen *önce ambulanslar gönderildi*. Daha sıradan yollarla, mağazalar indirimler sunmak için geçen müşterilerin tercihlerini tespit edebilir ve pazarlamacılar ürünleri cerrahi hassasiyetle tanıtabilir.

2026'nın akıllı evinde, kötü bir ruh hali içinde dolaşan birine, PFR ve EVM güdümlü, AI güdümlü sanal kapıcı (Siri, Alexa ve diğerlerinin çok daha akıllı ve daha insan torunları) tarafından yaklaşması muhtemeldir. ham, birinci nesil etkileşimli sistemler). ²⁴ "Bugün moralin bozuk görünüyor Jeremy," diyebilir o zaman:

En sevdiğin Çin yemeğini sipariş etmeme ne dersin? 23 dakikada burada yiyebilirim ve buzdolabının arkasında hâlâ bir Duvel birası var. Bu hafta yemek için ayırdığınız paranın hala 50 doları kaldı, sipariş için bolca. Ya da evinizdeki yiyeceklerle bir araya getirebileceğiniz onaylanmış sekiz tarif önerebilirim ve ben mutfakta güzel bir caz çalarken bunları birlikte inceleyebiliriz.

Bulut, bu tür milyonlarca etkileşimin sonuçlarını sürekli olarak toplayacak, elde edilen verileri ilişkiler için ayrıştıracak ve performansını yinelemek için ipuçları verecektir.

Bir eşin partnerinin yüz ifadelerine uyum sağlayabildiği, ruh halini ve tercihlerini sözlü iletişimin çok ötesine geçen şekillerde okuyabildiği aynı çok ince ayarlı ve sezgisel yolla, Bulut da bu tür bir uyumun makul bir kopyasını yapabilir. .

²⁴ Ortaya çıkan birkaç "dijital danışmanın" kısa bir açıklaması Signe Brewster'dır, "Bir Haftayı Chatbotlarla Yaşayarak Harcadım—Bütün Bu Kendi Kendine Yardım Etti mi?" *Kablolu*, 4 Ocak 2018.

Kritik çıkarım - on yıl önce zaten çok fazla kanıt var ama şimdi giderek yaygınlaşıyor - algoritmaların şimdi daha önce insan yargısına bırakılan binlerce sosyal karar alması gerçeğidir.

Bugün, bir genç küçük bir suçlamayla ilk kez tutuklandığında, onun cezasına karar verecek olan bir yargıç değil, bir algoritmadır. Birisi acil servise geldiğinde, sensörler binlerce veriyi toplayacak, bunları bireyin dosyadaki tıbbi kaydıyla birleştirecek ve ardından algoritmalar hastane personelini tedaviye yönlendirecek. AI güdümlü, VR etkileşimli sohbet robotları ile birleştirilen algoritmalar, birçok düşük seviyeli terapötik tedavi vakasında terapistlerin yerini almıştır. Bir şehrin refah bütçesinin ne kadarını hangi programlara ve koruyucu çocukların nereye yerleştirileceğine onlar karar veriyor. İpotek başvurularının yanıtlarını belirliyorlar ve 22-25 yaşlarında, 40-50 yaşlarında kimin mali açıdan sorumlu olacağını ve bu nedenle özel mali programlara erişim verilmesi gerektiğini giderek daha fazla *tahmin ediyorlar*.²⁵

Bu gelişen yetenek yelpazeyle donatılan The Cloud'un faaliyetleri, "pasif seçim ilkesi" veya POPE olarak bilinen temel bir fikri yansıtmaya başladı.²⁶ Yapay zeka programları, çeşitli konularda ne yapacağınıza, neye ihtiyacınız olduğuna veya ne düşündüğünüze dair doğru bir fikir veriyorsa,²⁷ neden bilinçli bir çabayla böyle bir karar verme zahmetine katlanıyorsunuz? ("Sadece Papa'nın dediğini yapın" diyor insanlar.) En basit örnek alışveriş: Bir zamanlar bildiğimiz bakkal artık geçmişte kaldı, yerini devasa depolara bıraktı.

25 Genel eğilim ve riskleri hakkında bkz. Danah Boyd, "Beyond the Rhetoric of Algorithmic Solutionism," *Data and Society: Points*, 11 Ocak 2018.

26 Bu kavram, kısmen davranışsal ekonomi üzerine yazılan yazılardan ve insanları "daha doğru" kararlar almaları için en iyi şekilde "dürtmek" üzerine yapılan analizlerden ortaya çıktı. Bu alanda yazan bilim adamları, örneğin olabileceklerinden daha az ilgi kazanmayı bilinçli olarak seçen insan "irrasyonelliklerini" katalogladılar ve bu anormallikleri ipuçları veya örtük etki ile "düzeltmeye" çalıştılar. Belirgin bir örnek, belirli seçmeli seçeneklerdeki varsayılan seçeneklerin değiştirilmesi - örneğin emeklilik için tasarruf etmek. Objektif olarak daha verimli sonuçları belirleme ve insan seçimini bunlara uyacak şekilde varsayma ilkesi, şimdi Bulut tarafından geliştirildi ve güçlendirildi.

27 Scott Magids, Alan Zorfas ve Daniel Leemon, "The New Science of Customer Emotions", *Harvard Business Review*, Kasım 2015.

Amazon tarafından işletiliyor. Büyük veriler, çoğu insanın haftalık yiyecek alımlarının yüzde 73 standart olduğunu gösterdi, öyleyse neden 19. yüzyıldan kalma bir bakkala gidip her hafta aynı sınırlı bozucu süreçten geçerek zamanını boşa harcıyorsun? Akıllı buzdolapları ve Amazon'un internet sitesindeki aynı "beğendiyseniz buna bayılacaksınız" ilkesi üzerinden deneysel satın almalar oluşturan tercih algoritmaları, insanların tercihlerini onlar adına yapıyor. Tüketiciler her zaman sistemi geçersiz kılabilir, ancak çok azı bunu yapar ve anketler müşterilerin yüzde 90'ının Bulut'un kendileri için verdiği kararlardan memnun olduğunu gösteriyor.

2016 civarında, bilgin Yuval Noah Harari bu zihniyeti "Vericilik" olarak adlandırmaya başladı. "Yeterli biyometrik veri ve bilgi işlem gücü verildiğinde," diye açıkladı, "her şeyi kapsayan bu sistem, insanları bizim kendimizi anladığımızdan çok daha iyi anlayabilir. Bu gerçekleştiğinde, insanlar otoritelerini kaybedecek ve demokratik seçimler gibi hümanist uygulamalar, yağmur dansları ve çakmaktaşı bıçaklar kadar demode hale gelecek." ²⁸ Bu yetki kaybı, milyonlarca ayrı biyokimyasal, nörolojik, davranışsal ve tutumsal veri noktasını saniye saniye toplama ve bunları algoritmik tabanlı tercihlere çevirme yeteneğine sahip sensörlerin bir kombinasyonu ile esasen meydana geldi. Vericiler haklı olarak Harari'nin endişelendiği gibi çoğu seçimde sistemin "duygularımı benden çok daha iyi anladığını" ve bu nedenle nesnel olarak daha doğru kararlar verdiğini iddia edebilirler. ²⁹ Örneğin, on yıl kadar önce, algoritmaların dijital egzozlarına dayanarak insanların kişilikleri hakkında insanlardan daha iyi yargılarda bulunabileceği tespit edildi. ³⁰

POPE, giyim, araba ve hatta evler gibi diğer satın alma kategorilerine genişletildi. Bulut çoğu zaman sizin ne istediğinizi sizden daha iyi bilir, çünkü kendi önyargılı karar motorunuzdan daha objektif bir tercih değerlendiricisidir. İlke, uzun zamandır çevrimiçi olan arkadaşlık sitelerinde yerleşmiştir.

²⁸ Harari, 2016.

²⁹ Harari, 2016.

³⁰ Wu Youyou, Michael Kosinski ve David Stilwell, "Bilgisayar Temelli Kişilik Yargıları, İnsanlar Tarafından Yapılanlardan Daha Doğrudur," *Proceedings of the National Academy of Sciences*, Cilt. 112, No. 4, 2015.

radikal olarak daha doğru ve etkilidir. Neredeyse hiç kimse, tavsiyelerine karşı olası bir eşle bağlantı kurmayı tehlikeye atmaz: Rakamlar birbirini tutmuyor. Match.com artık “yüksek güven” maçları için yüzde 37 “nihayetinde evlenme” rakamına sahip; veriler, flört partnerlerini manuel olarak seçen kişilerin yalnızca yüzde 2'sinin uzun süreli bir ilişki içinde olduğunu gösteriyor.

Bilgin Alex Pentland, ortaya çıkan bilimin bir versiyonunu “sosyal fizik” olarak adlandırdı: “bir yanda bilgi ve fikir akışı ile diğer yanda insanların davranışları arasındaki güvenilir, matematiksel bağlantıları tanımlayan nicel bir sosyal bilim.” Pentland'ın ifade ettiği gibi, yeni bilimin hırsları alçakgönüllüydü: “Haydi düşünelim,” diye hipotez kurdu, “tüm bir topluluğun etrafına bir görüntüleme odası yerleştirme ve ardından davranışın her yönünü ve boyutunu kaydetme ve gösterme yeteneği. üyeleri arasında iletişim ve sosyal etkileşim.”³¹ Daha enerji verimli topluluklar, daha sorunsuz ulaşım akışları, daha istikrarlı finansal piyasalar ve daha etkili tıbbi müdahaleler tasarlamak için insan sosyal davranışına ilişkin veriye dayalı tahminleri kullanmayı düşünüyordu.

Tüm bunlar, 2026'da, hatta onun “görüntüleme odası” geleceğinde öngörülen veri toplama derecesine çok yakın bir seviyede gerçekleşti. Ancak onun beklenen uygulamaları çok daha büyük bir şeyin parçası olarak ortaya çıktı: sosyal fiziğin giderek artan sayıda insan faaliyetine uygulanması.

İlke, ekonomik tercihlerin çok ötesindeki alanlara uzanır. POPE şeklinde ifade edilen Bulut, okul müdürlerine hangi çocukların hangi öğretmenlerle eşleşeceği konusunda talimat veriyor. Bir sonraki oyunu önermek için Ulusal Futbol Ligi (NFL) oyun kurucunun kulaklığına koç ya da hücum koordinatörü değil, o gelir. Duygusal tepkilere dayanarak, radyo istasyonlarına daha sonra hangi şarkıların çalınacağını söyler. Polis kuvvetlerine, en iyi suç önleme sonuçlarını elde etmek için dövülmüş polislerini nereye yerleştireceklerini söyler. *Azınlık Raporu* gibi bilim kurgu filmlerinde açıklanan “tahmini polislik”in ilk ipucunda, Bulut, gelecek hafta büyük bir suç işleme olasılığı yüzde 95'ten fazla olan az sayıda insanı belirleyebilir. . Bu tür insanlar artık rutin olarak alınıyor

³¹ Pentland, 2014, s. 4, 9.

ve uyardı, ancak toplum henüz suç öncesi niyetler için herhangi bir fiili cezayı kabul etmedi. ³²

Yenilikçi bilim adamları ve programcılar şimdi POPE'u siyasete yaymakla oynamaya başlıyor. Çoğunlukla, gelişmiş dünyanın siyasi kurumları, Bulut öncesi günlerde olduğu gibi işlemeye devam etti. (İnsanlar, olasılıksal konularda giderek daha ilkel, zaman alıcı ve verimsiz müzakereci yargılara “BTC [Bulutun Önce] Önemsiz” olarak atıfta bulunuyorlar.) yasama organlarının ve yöneticilerin süreçleri değişmedi. En büyük fark, hangi kararların alındığı konusunda olmuştur: Akıllı, veri ve yapay zeka güdümlü bir bulutun etkilerinden biri, politika alanını önemli ölçüde daraltması olmuştur. Bulut, eğitim, kanun yaptırımı, yoksulluğun azaltılması ve enerji güvenliği dahil olmak üzere yüzlerce sosyal konuyu teknik olasılık zorlukları haline getirdi. Pek çok alanda, toplumun kaynakları uygulama ve yargılarda bulunma biçimi olarak POPE, bilinçli, diyaloga dayalı kamu tercihinin yerini almıştır. Ve sonuçlar iyi ve ölçülebilir olduğu için insanlar genellikle bu sonuçtan memnun.

Şimdi, geri kalan açık siyasi kararları esasen POPE için takas etmek için öneriler var. Bulut, insanların seçimlerinin, davranışlarının, düşüncelerinin, ifade edilen fikirlerinin ve ima edilen inançlarının bir sosyal sistemde ne isteyeceklerini yüksek bir olasılıkla bilebilir. Ve bu tür tercihlerin en yüksek sayısının optimal tatminini yaratmak için algoritmalar oluşturabilir. Aslında, Kurucu Ataların çatışma ve uzlaşma yoluyla olacağına inandığı çıkarların rasyonelleştirilmesinin yapay zeka güdümlü otomatikleştirilmiş bir versiyonu olma potansiyeline sahiptir. Tüm bu rasyonelleştirme, maliyetler, dikkat dağıtıcı unsurlar, gerilimler ve bazen de açık bir siyasi sürecin doğrudan çatışması olmaksızın bir denklem içinde gerçekleşebilir. Sonunda, bakkaliye satın alırken olduğu gibi aynı seçeneği sunar: Bulut ne olduğunu biliyorsa

32 Rusya ve Çin gibi daha az açık ülkelerde durum çok farklı. Hükümetlerin suç işleme olasılığı yüzde 60 olarak uyarı barajı koyduğu ve yüzde 90'ın üzerinde olan herkesi tutuklayıp hapse attığı söyleniyor. Bu eşikler geleneksel suçlar içindir; siyasi sadakatsizlik için eşikler çok daha düşüktür.

insanlar sonunda tercih edecekler, neden bu tercihi yerine getirmek için gerekli adımları atması için yetki vermiyorsunuz?

Güvenlik Açıkları ve Riskler

Hatalar oldu ve emin olmak için riskler var. Herhangi bir büyük veri ağı hacklenebilir ve kâr amaçlı bilgisayar korsanları, Bulut'tan kaynakları sömürmek için mümkün olan her açığı kullandılar. FaceCoins ve AlphaCash çalışıyorlar; bakkallarla dolu sürücüsüz elektrikli kamyonları karaborsa dağıtım noktalarına yönlendirmek; ve kişisel verileri alın ve onlarca yıldır olduğu gibi kimlik hırsızlığını körüklemek için kullanın. Özellikle önemli bir eğilim, birbirine bağlı Bulutun büyük parçalarını (tipik olarak IoT'ye bağlı şeyler) kilitlemek için güçlendirilmiş fidye yazılımı saldırılarının kullanılması ve bireysel kullanıcıları veya büyük şirketleri bilgilerin kilidini açmak için büyük meblağlar ödemeye zorlamak olmuştur.

Yine de, genel olarak, sistem birçok kişinin korktuğundan daha dayanıklı olduğunu kanıtladı. Bu dayanıklılık iki şeyin ürünü olmuştur. İlk olarak, ağı çok yoğun olması ve birbirine bağlı olması onu daha az savunmasız hale getiriyor. Çok az sayıda tek hata noktası ve birçok yedekleme sistemi ve yeteneği vardır. İkincisi, en güçlü AI gelişmeleri, beş büyük firmaya aittir ve Bulut'un istikrarını korumak için dağıtılır. Onu baltalamak veya ondan çalmak için çeşitli çabaları öngörür, sezer ve peşine düşerler. Sonuç mükemmel değil ama büyük ölçüde yeterince iyi oldu.

The Cloud'un bir başka riski veya popüler güvenlik açığı, giderek artan bir şekilde bireysel özgürlük üzerindeki bir dizi kısıtlamayı yansıtması duygusu olmuştur. Gelişmiş demokrasilerin vatandaşları, giderek bu algoritmik gerçekliğin yönlerini, Çin'in kötü şöhretli “sosyal kredi puanı”nın uğursuz, hafifçe yumuşatılmış versiyonları olarak görmeye başladılar: bir kişinin ekonomik ve politik açıdan güvenilirliğini yansıtan acımasızca basitleştirilmiş bir sayı.³³ Amerika Birleşik Devletleri'nde bile, krediler ve işler de dahil olmak üzere, en iyi okullar, doktorlar ve hastaneler de dahil olmak üzere temel sosyal hizmetlere erişim caydırıcıdır.

³³ Sosyal kredi puanının nasıl çalıştığına ilişkin bir açıklama için bkz. Mara Hvistendahl, “Inside China's Vast New Experiment in Social Ranking,” *Wired*, 14 Aralık 2017.

İnsanların yaşam boyu süren davranışlarının sayısal temsilleri ile çıkarılır, işlemleri genellikle kamunun incelemesine kapalı olan veri tabanlarında saklanır. İnsanlar anlamadıkları nedenlerle evlerinden, işlerinden ve üniversiteye kabullerinden mahrum bırakılıyor. Bu eğilime karşı halkın tepkisi büyüyor ve bu algoritmik karar verme gerçekliğinin büyük bir kırılğanlığını yansıtıyor.

Bu eğilim, Bulut'un hizmet ettiği topluluklarla ilişkisiyle ilgili daha büyük zorlukları yansıtıyor. Böyle bir meydan okuma, sistem ile suçluları ve sabotajcıları arasındaki ortak yaşamdır. Birkaç aşırı neo-anarşist bilgisayar korsanı, Bulut tabanlı sistemin tamamının kötü olduğuna ve yıkılması gerektiğine inanarak kendilerini günümüzün Unabomber'ları olarak nitelendiriyor. Bununla birlikte, çoğunlukla, daha akıllı bilgisayar korsanları, başarılarının işleyen ağlara *bağlı olduğunu bilirler*. Temel hedefleri konusunda bilinçlidirler: Bulut'un temel bütünlüğünü tehdit etmeden kendilerini zenginleştirecek kadar tepeden tırnağa kaymak.

Kâr amaçlı yeni bir kötü amaçlı yazılımın Bulut üzerinden beklenmedik ve tehlikeli şekillerde yayılmaya başladığı ve ardından siber güvenlik firmalarının solucanları en iyi şekilde nasıl devre dışı bırakacakları konusunda gizemli talimatlar aldığı yüzlerce belgelenmiş vaka var. Güvenlik görevlileri ve bilgisayar korsanları arasındaki ilişki, Soğuk Savaş'ın sonlarında ABD-Sovyet ilişkilerinin bazı özelliklerini üstlendi: düşmanca ama yoğun bir resmi ve gayri resmi kurallar ve normlar ağı tarafından yönetiliyor ve bir dereceye kadar kişisel ilişkilerle istikrara kavuşuyor (olsa bile). gerçek kimlikleri korumak için genellikle sanal) ve önemli derecede karşılıklı saygı.

Yine de, herhangi bir mahremiyetin yokluğundan endişe duyan artan sayıda insan, gerçek benliklerinin birçok yönünü gizli bırakırken, çevrimiçi avatları Bulut tabanlı kişilikleri olarak kullanmaya başladı. Bu avatlar "Yankılar" olarak bilinir hale geldi. Böyle bir avatar, tamamen yararsız reklamlar, teklifler ve bilgilerden oluşan büyük bir akış oluşturmamak için gerçek kişinin belirli özelliklerini yansıtır, ancak kilit yönlerden farklıdır: yani gerçek kişinin bir "yankı". Dark web, birincil veritabanlarına gömülü ve kişisel bilgilerle (örneğin, doğum belgeleri, vergi beyannameleri ve okul transkriptleri) eksiksiz olarak tamamlanmış Yankılar satan sitelerle doludur; uzun vadeli tarama ve satın alma kayıtları; hayali bir adres ve bütün

ikamet geçmişi; soy web sitelerine eklenen aile öyküleri; ve hatta fabrikasyon görünüm—görüntü oluşturma yazılımıyla oluşturulan ve yüz tanıma veritabanlarına sızan yüzler, bu icat edilmiş “kişinin” çeşitli şehirlerde dolaşıyormuş gibi görünmesini sağlar.

Bununla birlikte, bugüne kadarki en büyük risk, seçimin otomasyonu ile sonuçlanan bu tür teknolojilerin, Amerikalıları çok çeşitli konularda lehte ve aleyhte gruplara ayıran meçhul bir kovan zihni yaratmasıdır. Teknoloji eşitsizliği artırıyor çünkü yalnızca geçmiş performansın gelecekteki sonuçlara nasıl rehberlik etmesi gerektiğine bakabiliyor. Tesadüfi, yörünge değişikliği veya değişim potansiyelini açıklayamaz ve yerleşik kalıplarla eşleşmeyen aykırı değerleri açıklayamaz. Sonuç, kişinin birikmiş itibarından kaçmanın görünüşte daha da zorlaştığı, otomatikleştirilmiş bir seçim dünyasında sosyal bölünmeleri sertleştirmek oldu.

Algoritmik Bir Gelecekte Bilgi Saldırganlığı

Bu gelecekte enformasyona dayalı saldırırganlığın birincil yolu, toplumun sayısallaştırılmış karar kollarının doğrudan manipölasyonu olmuştur. Ortaya çıkan bu gerçeklik, basit dezenformasyon veya siber saldırıdan çok daha sinsi, dolaylı bir saldırırganlık biçimine izin veriyor: Saldırırganlar, sistemleri bozmak için kötü amaçlı yazılım kullanmak üzere tasarlanmış müdahaleler yerine, insan yaşamının çoğunu yöneten algoritmaları hacklemeyi umuyorlar. Amaç, haftalarca veya aylarca fark edilmeyecek, sonuçları zararlı şekillerde çarpıtan ve operasyonun çarklarına kum fırlatan, sosyal hayal kırıklıklarını şiddetlendiren ve tutumları etkileyen küçük ince ayarlar yapmaktır.

Son yıllarda sağlık hizmetleri, insan kaynakları, internet aramaları, adalet ve sosyal medya platformları gibi sektörlerde bir dizi “algonun ayarlanması” saldırıları görüldü.³⁴ Bugüne kadar bilgi güvenliği firmalarının bu tür binlerce değişikliğin gerçekleştiğine inanılmaktadır.

³⁴ Bu tür saldırılarda uzmanlaşan bilgisayar korsanları, "ayarlayıcılar" olarak bilinir hale geldi. Karanlık ağda, tunerlerin teknikleri, algoritmik sistemlerin güvenlik açıklarını ve başarı hikayelerini paylaştığı, bu uygulamaya özel olarak ayrılmış siteler vardır.

birkaç azınlık adayını değerlendirme dışı bırakmaya çalışan bir işe alma algoritmasının programlanmasında bir değişiklik de dahil olmak üzere sadece birkaç düzine kanıtladı; binlerce yanlış pozitif teşhis üreten bir kanser tarama algoritmasının kodunda bir değişiklik; Reform potansiyeli yüksek olanlara uzun, yeni suç işleme olasılığı yüksek olanlara çok daha kısa cezalar önermeye başlayan, ilk kez suçlular arasında tekrar suç işlemeyi tahmin etmek için kullanılan bir algoritmada yapılan değişiklikler.

Bu kampanyalar hem devlet hem de devlet dışı aktörler tarafından üstlenildi. Gerçekten de, atfetmeyle ilgili endişeler nedeniyle, ulus devletlerle doğrudan bağlantılı kuruluşların bu tür tekniklerle diğer devletlere doğrudan saldırması çok nadirdir. Bunu yapmaya hiç gerek yok: Devletlerin emrinde, özel aktörleri yönlendirmeden onlara ilham vermek için muazzam bir dizi devlet dışı milis, hacker kolektifi, vatansever siber ekipler, kâr amaçlı siber özel şirketler ve kitle kaynak kullanımı ve benzeri teknikler var. Keşfedilen algoritmaların çoğu manipülasyonu, bu tür özel aktörlere kadar uzanır; bir avuç tutuklandı ama çoğu cezasız kaldı. Bu fırsatlar, Amerika Birleşik Devletleri'ne düşman güçlerin küresel bir sosyal manipülatörler ağını bir araya getirmeleri için bir yol sundu; dünya çapında ABD'nin gücünü kısıtlamaya adanmış ve yarı devletten eğitim, ilham ve bazen yönlendirme alan on binlerce insan. varlıklar.

Bu saldırı dalgasının bir sonucu, kural olarak, algoritmik karar verme konusunda halkın güvenini sarsmak olmuştur. Bu sistemlerin birçoğu saldırıya uğradığından, diğerlerinin çoğunun doğruluğu sorgulandı. Bu inanç eksikliği, pek çok algoritmanın "kara kutu" karakteriyle daha da kötüleşiyor: Karar verme süreçlerinin derin öğrenme yoluyla geliştirildiği durumlarda, programın kendisi altta yatan ilişkileri geliştirdi ve programcılar bunun nedenini bile bilmiyorlar. bazı sonuçlara varır. Diğer durumlarda, iyi anlaşılan algoritmaların bile işleyişi, özel ticari sırlar olarak tutulur ve gerçek koşulları hakkında komplo teorilerini körükler. Bu programlarda genel bir güven kaybına yol açmak için dışarıdan düşmanca bir manipülasyona pek gerek kalmamıştır.

Bu saldırılar dizisinin sonucu, özellikle gelişmiş demokrasilerin karakteristik özelliği haline gelen karar vermenin doğasında bulunan sosyal güveni daha da tehlikeye atmak oldu. Yıllar boyunca vatandaşlar hayatlarının giderek daha fazla algoritmalar tarafından ele geçirildiğini gördüler; şimdi, bu programların düzenli olarak tehlikeye atıldığından ve yerel veya yabancı düşman aktörler tarafından manipüle edildiğinden giderek daha fazla eminler. Bu gerçeklikteki bilgi küresinin doğası göz önüne alındığında, bu eğilimlerin sosyal ve kurumsal güven düzeyi üzerinde yıkıcı etkileri oluyor ve postmodern ileri demokrasinin temel özelliklerine karşı artan şikayetlere neden oluyor.

Sanal Toplumsal Savaşın Ortaya Çıkan Riski

Önceki bölümlerde açıklanan üç gelecek, ortaya çıkan bilgi dünyası ve bununla bağlantılı bilgi tabanlı saldırganlık riski hakkında kapsayıcı bir gerçeğe işaret ediyor: Mevcut birçok eğilim, gelişmiş demokrasilerin bilgi ortamında benzeri görülmemiş güvenlik açıkları üretiyor. Bu, bilgi dünyasındaki hızlanan eğilimlerin, tutumlar ve güven hakkındaki sosyal bilim derslerinin ve bilgi manipülasyonu ile ilgili hızla gelişen bir dizi teknolojinin potansiyelinin birleşik sonuçlarından çıkarılacak özet çıkarımdır. Gelişmiş demokrasiler, günlük faaliyetleri ve vatandaşlarının kaderi ve esenliği için, çoğu otomatikleştirilmiş veri tabanları ve bilgi işleme temeline giderek daha fazla bağımlı hale geliyor. Ancak, fiziksel hedeflere yönelik geleneksel siber saldırı senaryolarının çok ötesinde, devlet ya da devlet dışı düşman aktörler, önümüzdeki yıllarda bu bilgi temellerini bozmak ve bozmak için artan fırsatlara sahip olacaklar.

Özgür toplumlar özünde “bilgi işleme mekanizmaları”dır. 1 Ekonomik pazarları ve siyasi süreçleri, çeşitli bilgi türlerinin etkin, güvenli bir şekilde ele alınmasına ve değerlendirilmesine dayanır. Gördüğümüz gibi, sosyal güven, diğer insanların ve sosyal kurumların doğru algılanmasına bağlıdır. Bununla birlikte, bu işleme sistemlerinin doğası, bilgi dünyası ile birlikte değişmektedir. Özgür toplumlar uzun zamandır geniş ve kavramsal anlamda bilgi işleme mekanizmaları olmalarına rağmen, giderek daha fazla hale geliyorlar.

1 Braden R. Allenby, “Silahlaştırılmış Anlatı Çağı veya Nereye Gittiniz Walter Cronkite?” *Bilim ve Teknoloji Sorunları*, Cilt. 33, Sayı 4, Yaz 2017, s. 68.

gerçek, genellikle otomatik ve bazen tamamen gizemli yollar. Ortaya çıkan bilgi dünyasının karakteri, düşman aktörler bu mekanizmaların işleyişini bozmak için vitese geçmeden önce bile toplumsal güven ve istikrar için yeterince zorlayıcıdır.

Diğer büyük güçler, bilgi ortamının manipülasyonunu ulusal rekabet için önde gelen bir strateji olarak açıkça görmektedir. Rus siber doktrininin 2011 tarihli bir beyanı, sadece bir örnek vermek gerekirse, “bilgi sistemlerine, süreçlere ve kaynaklara” saldırmak için çaba gösterilmesini, aynı zamanda düşmanın “siyasi, ekonomik ve sosyal sistemini” baltalamak ve “büyük beyin yıkama” yaratmak için çağrıda bulunuyor. toplumu ve devleti istikrarsızlaştırmak için nüfusun 2 Demokrasilerin bilgi temellerine karşı giderek genişleyen saldırganlık teknikleri büyük bir rekabet avantajı olarak görülebilir.

Rakiplerin toplumlarına bozulma amacıyla doğrudan müdahalenin ötesinde, liberal olmayan rejimler, iddia edilen vatandaşlar, kültürel arkadaşlar veya sadece bir arkadaş ya da ilgi alanı haline gelen herkes dahil olmak üzere dünya çapındaki nüfusları etkilemek, zorlamak ve korkutmak için giderek sınırlarının ötesine geçer. düşman. Rusya, Çin, İran ve diğer ülkeleri eleştirenler artık rutin fiziksel taciz ve çoğu durumda dünyanın herhangi bir yerinde kaçırılma ve kaybolma ile karşı karşıya. 3 Bilgi-küreleri aracılığıyla diğer toplumlara ulaşma yeteneği, liberal olmayan devletlere gözetim ve yıldırma taktiklerini benzeri görülmemiş şekillerde evrenselleştirme konusunda eşi görülmemiş bir yetenek sunar.

Bu çalışma, zorlama ve manipülasyonun bilgi mekanizmalarına odaklanmış olsa da, bir ülkenin bilgi dünyasına yönelik bu tür saldırılar, giderek daha fazla fiziksel veya daha kinetik tekniklerle birleştirilebilir ve yine de doğrudan saldırganlık olarak kabul edilebilecek olanın gerisinde kalır. Açık bir örnek, Rusya'nın son yıllarda Avrupa'da kimyasal ve biyolojik silah kullandığı iddiasında olduğu gibi, rejim karşıtları gibi belirli kişilerin geleneksel olarak gizlice hedef alınmasıdır. Diğer örnekler yakında otonom kullanımı içerebilir.

2—Segal, 2016, s. 112.

3 Bkz. Osnos, 2018.

bireyleri veya yerleri yüksek oranda hedef alan doğrudan drone tabanlı saldırılarda böceklerin boyutunu (veya nihayetinde daha da küçük) sistemler. 4

Yeni Bir Çatışma Biçimi: Sanal Toplumsal Savaş

düşmanca sosyal manipülasyondan daha kapsayıcı ve düşündürücü bir terime duyulan ihtiyacı ortaya koydu . Ortaya çıkan şey, bu terimden daha kapsamlıdır. Devletler ve devlet dışı aktörler, giderek artan bir şekilde diğer toplumlara ulaşma ve büyük savaşlar veya hatta herhangi bir kinetik eylem dışında önemli aksamalara neden olma yeteneğine sahiptir, çünkü bu tür eylemler örneğin Birleşmiş Milletler Şartı'ndaki silahlı çatışma tanımlarını karşılayacaktır. . Yine de potansiyel faaliyetler, propagandanın, hedefli pazarlamanın veya sosyal manipülasyonun diğer ikna edici yönlerinin dar sınırlarının çok ötesine geçer.

Ortaya çıkan gerçekliği yakalamak için *sanal toplumsal savaş* terimini öneriyoruz . Bu savaş, rakip ulusların sosyal istikrarına saldırmak için büyük ölçüde kinetik olmayan, bilgiye dayalı saldırganlığın kullanılmasını içerir. Sanaldır çünkü *çoğunlukla* bu stratejiler doğrudan fiziksel şiddet veya yıkım kullanmaz. (Dolayısıyla bu kavram, hem doğrudan askeri saldırıları hem de bir ülkenin fiziksel altyapısına zarar vermek ve gerçek hasara neden olmak için tasarlanmış büyük ölçekli siber saldırıları hariç tutar.) *Toplumsaldır* çünkü bu tür kampanyaların hem hedefleri hem de katılımcıları geniş kapsamlıdır. hedef toplumun verimli işleyişini, güven seviyelerini ve nihayetinde hedef toplumun istikrarını baltalamak olduğu için. Ve bu *savaştır* , çünkü potansiyel olarak daha ayrıntılı biçimlerinde, yalnızca devam eden bir rekabette göreceli avantaj elde etmek için değil, aynı zamanda hedefi terk eden yollarla kesin zafer kazanmak için rakip uluslar üzerinde üstünlük sağlamak için tasarlanmış bir faaliyeti temsil eder. ulus, saldırganın iradesine tabidir.

Önceki bölümlerin önerdiği gibi, sanal toplumsal savaş, ortaya çıkmakta olan savaşın karakteri bağlamında birçok biçim alabilir.

4 Evans, 2015.

bilgi küresi. Diğerlerinin yanı sıra aşağıdaki tekniklerin herhangi bir kombinasyonunu içerebilir:

- Sosyal bilim araştırmalarından tutum ve tutum değişikliği hakkında bildiklerimize rağmen, sosyal medya da dahil olmak üzere birden fazla kanal aracılığıyla klasik propaganda, nüfuz ve dezenformasyon operasyonlarını uygulamak, bu operasyonların yoğunlaştırılması için nüfusun alt bölümlerini hedefleme biçimini alması muhtemeldir. Bir popülasyonda toptan yeni inançlar yaratmaya veya değiştirmeye çalışmak yerine bölünmeler ve kutuplaşma
- paylaşılan gerçekliğe olan güveni azaltmak için büyük miktarlarda son derece makul fabrikasyon video ve ses materyali üretmek
- doğru ve yanlış bilgi arasında ayrım yapabilen kilit aracı kurumların itibarını sarsmak
- ekonominin ana bileşenlerinin giderek daha fazla güvendiği veritabanlarını bozmak veya manipüle etmek
- Algoritmik karar alma sistemlerini manipüle etmek veya aşılacak, hem günlük hükümet ve şirket operasyonlarını bozmak hem de kurumlara olan inanç kaybını, sosyal şikayetleri ve kutuplaşmayı yoğunlaştırmak için
- Bozulma veya zihinsel ıstırap yaratmak veya belirli anlatıları güçlendirmek için VR ve AR sistemlerini ele geçirmek
- verimsizlik ve bazı durumlarda kişisel hayal kırıklığı ve endişe yaratmak için sohbet robotu tarzı etkileşimli sistemlere komutlar eklemek.

Tam kapsamlı sanal toplumsal savaşta, bu bilgisel bileşenlere başka araçlar ve teknikler de katılabilir. Bunlar, doğrudan siyasi savaş ve bir hedef ülkede aktif beşinci kol oluşturmak için tasarlanmış, belki de yukarıdaki teknikleri kullanarak devletin diasporasından veya etnik olarak bağlantılı topluluğundan alınan gizli operasyonları içerebilir. Bunlar, mikroskobik insansız hava araçları veya kişiselleştirilmiş biyolojik silahlar ve diğer birçok saldırı biçimi aracılığıyla rakipler veya düşman için büyük önem taşıyan bireylere yönelik hedefli suikastlar da dahil olmak üzere daha kinetik siber saldırıların kullanımını içerebilir.

Sanal toplumsal savaşın, birlikte bu yeni savaş biçiminin temel doğasını ve karakterini yansıtan birçok temel özelliğe sahip olması muhtemeldir. Bunların tam olarak anlaşılması ancak zamanla ortaya çıkacaktır, ancak bu analiz, ortaya çıkan bu zorluğu tanımlamaya ve kavramaya yardımcı olabilecek bir dizi başlangıç özelliğine işaret etmektedir. Aşağıdaki bölümlerde açıklanmıştır.

Ulusal güvenlik, giderek daha esnek bir bilgi ortamına ve daha da temel olarak güçlü bir sosyal topografyaya dayanacaktır. unsurları Esnek bir bilgi dünyası iyi anlaşılmamıştır, ancak muhtemelen klasik bilgi güvenliği biçimlerinin yanı sıra güçlü aracı kurumları ve sosyal manipülasyon tekniklerine karşı güçlü bir şekilde aşılınmış bir nüfusu içerirler. Amerika Birleşik Devletleri ve diğer birçok gelişmiş demokrasi, bilgi güvenliğinde bazı ilerlemeler kaydetmiştir, ancak hiçbir yerde gerçek dayanıklılığa yakın değildir. Yıkıcı anlatıları şekillendirme ve inşa etme çabalarına karşı dirençli bir nüfus ve bilgi ortamı yaratmak için kayda değer bir çaba gösterilmedi. Bazı bilgi saldırı biçimleri için bilgi güvenliğinin yanı sıra bilgi müdahale kaynaklarına giderek daha fazla ihtiyaç duyulabilir: Örneğin, biri tedavi amaçlı sohbet robotunun kaçırıldığına ikna olduğunda kime gidecek?

Pentland'ın “sosyal fizik” kavramı –bireysel davranış ve sosyal sermaye unsurları arasındaki ilişkiler ve bunların birbirleriyle ilişki kurma biçimleri– sanal toplumsal savaş alanının en iyi kavramsallaştırmalarından birini sunar. Bilgi bilimi uzmanı ve uygulayıcısı Tim Hwang, konuyu bir ulusun *sosyal topografyasını* , dış hatlarını ve zayıf noktalarını değerlendirme ve yönetme konusundaki bir zorluk olarak açıkladı . 5 Bu topografyanın güçlü ve zayıf yönlerinin, ortaya çıkan tehlike alanlarının ve direnç kaynaklarının haritasını çıkararak anlamak, demokrasilerin giderek artan bir meşguliyeti haline gelecektir. Ancak nereden başlayacağımız veya böyle bir toplumda görevden hangi ofis veya kurumun sorumlu olması gerektiği konusunda bile hiçbir fikrimiz yok.

Kamusal ve özel çabalar ve sorumluluklar arasındaki engel bulanıklaşıyor; ulusal güvenlik, özel sektör işbirliğine dayanacaktır.

5 Tim Hwang, *Manevra ve Manipülasyon: Çevrimiçi Bilginin Askeri Stratejisi Üzerine Warfare* , Carlisle Kışlası, Pa.: Stratejik Araştırmalar Enstitüsü, 2019.

aktörler kadar kamu yatırımları da Önceki bölümlerde belirtildiği gibi, Bu tür bir çatışmanın teknolojileri ve teknikleri, çok çeşitli aktörler için giderek daha fazla erişilebilir hale geliyor. AI, propaganda ve etkileşimli botların otomatik olarak yerleştirilmesine izin verdiği için bu daha da doğru olacak. Bu alandaki özel güç, bazı durumlarda kamu gücünü aşar ve aşar.

Sonuç olarak, bu zorluğa verilen yanıtlar da giderek özel sektörün rolüne bağımlı hale geliyor. "Amerika'nın kamusal konuşmalarının çoğu, kimin kimi etkilemek için ne yaptığını kimsenin bilmediği, özel sektöre ait alanlarda gerçekleşiyor." ⁶ Kamu ve özel kurumların, gelişmiş demokrasilerin güvenliğini korumak için derin ve sürekli yollarla işbirliği yapması gerekecektir.

Benjamin Wittes ve Gabriella Blum, çatışmanın değişen doğasına ilişkin zorlayıcı analizlerinde sonucun, kademeli bir "hukukta, uygulamada ve önemli güvenlik işlevlerinin geleneklerinde - gözetim, analiz, müdahale ve hatta kıyı şeridi—hükümetten özel aktörlere." Bu, "saldırıların ve diğer güvenlik tehditlerinin gerçekleştiği ve saldırılara karşı savunmasızlığın kendisini ifade ettiği mimari üzerindeki fiili kontrolde temeldeki bir kayma nedeniyle" oluyor. Eskiden Amerika'ya saldırmak için onun kıyılarına asker çıkarmak ya da toprakları üzerinde uçak uçurmak gerekiyordu." Şimdi ise bunun tersine, "kişi Amerika'ya -ya da herhangi bir ülkeye- çeşitli biçimlerde saldırabilirken, yalnızca çeşitli türlerdeki özel şahısların sahip olduğu ve işlettiği mimariyle etkileşime girebilir." ⁷

Bu gelişmeler, devletin toprak güvenliğinin sağlayıcısı olarak geleneksel rolünü zayıflatacaktır. Bu rol, onun en temel yükümlülüğüdür, ancak savaş kanallarının ordular tarafından savunulmadığı, ancak şirketler, sosyal medya platformları ve sosyal medya platformları tarafından savunulması gereken sanal bir toplumsal saldırganlık dünyasında giderek daha fazla yerine getiremeyeceği bir roldür. önemli haber kaynakları. Bu gelişmeler, özellikle geleneksel olarak açık toplumlar için sorunludur.

⁶ Henry Farrell, "American Democracy Is a Easy Target," *Foreign Policy* , 17 Ocak 2018.

⁷ Benjamin Wittes ve Gabriella Blum, *Şiddetin Geleceği: Robotlar ve Mikroplar, Hackerlar ve Drones* , New York: Basic Books, 2015, s. 79-80.

kamu ve özel sektör arasında güçlü bir engel oluşturdu ve Çin gibi toplumun bu tür unsurlarını harmanlayan hükümetlere avantajlar sunabilir.

Çatışmalar ağlar arasında ve ağlar arasında artarak devam edecek . Wittes ve Blum, sanal toplumsal savaşla ilgili eğilimlerin bir çıkarımını "çoktan çoğa" güvenlik etkileşimleri modeli olarak tanımladılar. Her ulus, şirket, grup ve birey diğerlerini tehdit edebilir, yazıyorlar. "Bu nedenle, dünya tarihindeki hiçbir şeye benzemeyen, mesafelerin sizi korumadığı ve aynı anda hem büyük bir güç hem de büyük bir kırılabilirlik figürü olduğunuz bir andayız." ⁸

Sonuç, ağların ağlara karşı savaşıdır. "Devletler, çok sayıda ortak kuruluş kullanarak gelecekteki savaşlarla giderek daha fazla savaşacaklar." ⁹ Bu model, örneğin, Rusya tarafından bilgi kampanyalarının bir parçası olarak istihdam edilen karmaşık, uluslararası bilgisayar korsanları, aktivistler ve gayri resmi propagandacılar ağında ve Çin'in Çin vatandaşlarını ve yurtdışındaki etnik Çinlileri kontrolünü ilerletmek için kullanmasında ortaya çıkıyor. anahtar anlatılar üzerinde. Devlet aktörlerinin, atıf yapmaktan kaçınmak ve aynı zamanda misillemeye karşı sanal toplumsal savaş yeteneklerini güçlendirmek için bu tür ağlar geliştirmesi muhtemeldir: Anlaşılması, doğru bir portresini sürdürmesi ve gölgeli bir küresel ağa karşı tepki vermesi çok daha zor olacaktır.

Bugün, bu ağ bağlantılı çatışma modelinin bir başka anlamı daha belirgin hale geliyor: kilit güvenlik işlevlerine yönelik "özelleştirme" yaklaşımı olarak adlandırılan yaklaşımın yükselişi. Wittes ve Blum, "Özel kişiler kendi operasyonlarını finanse ettiler ve ele geçirdikleri 'ödülleri' koruyarak para kazandılar," diye açıklıyor. "Tam olarak bu ademi merkezîyetçilik nedeniyle, özel sektör, özel sermayeyi, özel enerjiyi ve özel riski kamu askeri hedeflerinin hizmetinde toplamak için bir araç haline geldi." Bu model, yalnızca bir ulusun bilgi ağlarının sağlığını sürdürmek için özel bilgi güvenliği firmalarının kullanımında değil, aynı zamanda bilgisayar korsanlarının fidye yazılımlarını ve diğer teknikleri kullanarak kar elde etme modelinde ortaya çıkıyor.

⁸ Wittes ve Blum, 2015, s. 120.

⁹ Wittes ve Blum, 2015, s. 120.

faaliyetler. Böyle bir modele eşlik eden bir risk, ulusal güvenlik adına ihtiyatlılıktır. ¹⁰

Böyle bir ademi merkeziyetçilik sürecinde, güvenlik işlevi üzerindeki hükümet tekeli, yerini “dağıtılmış bir savunma işlevine” bırakıyor. Bu fikir

toplumların kendilerini dış ve iç tehditlere karşı en etkin biçimde nasıl örgütlediğine dair yüzyıllardır süregelen gelişmiş anlayışla çelişir. Bunu genellikle, çok sayıda aktör aracılığıyla gücü yayarak yapmazlar - çok daha fazla sayıda hissedarlara (yabancı hissedarlar dahil) karşı sorumlu olan özel aktörler çokluğu bir yana. ¹¹

Özel aktörler, hükümetin güvenlik işlevleriyle ayrılmaz bir şekilde bağlantılı hale gelir. Bu model, ulusal güvenlikten çok, "kendilerini sağlık ve güvenlik işinde görmeyen çeşitli aktörlere rutin olarak yükümlülükler dağıtmayı içeren" halk sağlığı ve güvenliğine benziyor. ¹² Araba, şekerleme ve alkol üreticileri, kamu sağlığı ve güvenliğine katkıda bulunan eylemlerde bulunmak üzere düzenlenir ve teşvik edilir; Gittikçe daha fazla sosyal medya platformları, geleneksel medya kuruluşları, eğlence şirketleri, internet sağlayıcıları, üniversiteler ve diğer kurumların sağlam bir bilgi dünyası ve sosyal topografya yaratmak için teşvik edilmesi gerekecek.

Bu dağıtılmış ağ modelinin, bu yeni çatışma biçimini kontrol etme ve düzenleme çabalarını karmaşık hale getirmesi muhtemeldir. Birçoğu özel ve bağımsız aktörler olarak faaliyet gösteren bireylerin artan zarar verme yeteneğinin varlığı, normların uygulanmasını çok daha zor hale getirecektir.

Bunlar, sanal toplumsal alanda çatışmayı yönetecek ilke türlerinin yalnızca ilk üç önerisidir. Bu alanı daha tam olarak anlamak ve anlamaya başlamak için acilen daha fazla araştırmaya ihtiyaç vardır.

¹⁰ Wittes ve Blum, 2015, s. 84, 87.

¹¹ Wittes ve Blum, 2015, s. 83.

¹² Wittes ve Blum, 2015, s. 81, 83–84.

demokratik toplumları en kötü etkilerine karşı koruyacak tepki türlerini anlayın.

Sanal Toplumsal Saldırganlık Tehdidiyle Başa Çıkmak

Bu analiz, düşmanca sosyal manipülasyonun geleceğine odaklandı ve bu süreçte, daha geniş sanal toplumsal saldırganlık riskini ciddiye almak için davayı yaptı. Bu çalışma aşaması, ayrıntılı bir politika tavsiyeleri gündemi geliştirmek için tasarlanmamıştır ve öyle de yapılmamıştır. Bununla birlikte, özellikle Amerika Birleşik Devletleri dahil olmak üzere ileri demokrasilerin burada özetlenen tehlikelerle başa çıkmak için değerlendirmeye başlaması gereken geniş tepki kategorileri için bir avuç açık yönü işaret ediyor.

Sanal toplumsal savaşın zorluğu, yalnızca yabancı aktörlerin faaliyetlerinden çok daha büyük bir toplumsal sorundur. Bütün bir kumaştan yenileri üretilmek yerine, önceden var olan sosyal problemler büyütülüyor. Amerika Birleşik Devletleri'ndeki kutuplaşma ve sosyal gerilimin derecesi, başkalarının onsuz sahip olamayacakları etkiye sahip olmaları için yollar sağlıyor. Ancak bu devasa, temel toplumsal sorunlar, yalnızca semptomlarına, yani ülkelerin bilgi ortamlarının manipülasyonu ve bozulmasına yönelik politikalarla çözülemez. Çok daha zor - ve genellikle daha tartışmalı - bir görev oluşturan temel nedenler ele alınmalıdır.

Böyle bir görevi üstlenen demokrasilerin, sanal toplumsal savaşta başarının nasıl görüldüğüne karar vermesi gerekecek. Başarı, kamusal tartışmalarda yalanların olmaması veya mükemmele yakın bir kamuoyu farkındalığı ile tanımlanamaz: Bu tür şeyler hiçbir zaman var olmadı ve demokrasiler onlarsız gayet iyi işliyor. Yeni ortaya çıkan AI, VR veya AR teknolojilerinin herhangi bir şekilde hacklenmesi olamaz. Şimdiki zor sorular, demokratik bilgi ortamlarının ne kadar istikrarsızlığa yol açabileceği ve sınırların nerede çizilmesi gerektiğidir. Bunlar kaçınılmaz olarak nitel yargılar olacaktır. Genel olarak konuşursak, hedef muhtemelen bireyler üzerindeki etkilerin dengelendiği ve dezenformasyonu belirleme ve azaltma tekniklerinin etkili olduğu bir tür denge olacaktır.

Herhangi bir politika yanıtını bilgilendirmesi gereken bir içgörü, bu daha büyük zorluğun arkasındaki nedensel dinamikler, ortaya çıkma biçimleri veya en büyük farkı yaratacak tepkiler dahil olmak üzere şu anda çok fazla şey bilmediğimizdir. Sorun acil olsa da, yanıtları formüle etmede yavaş gitmek yine de işe yarayabilir. Bunu çözdüğümüzü veya yapılacak doğru eylemleri bildiğimizi varsaymamalıyız.

Sadece bir örnek olarak, bilgi ortamlarının esnekliğini korumanın bir yolu olarak, sahte veya yanlış raporların aktif olarak düzenlenmesi, pratik sorunların yanı sıra birçok tehlikeyi de beraberinde getirir. Tarih, bariz bir risk önermektedir: Bir kez kurulduktan sonra, gerçekleri düzenleme yeteneği kötüye kullanılacak ve o sırada iktidarda olan herkes tarafından uygunsuz gerçekleri caydırmak için kullanılacaktır. Bu tür faaliyetler, seçmenlerin önemli bir kısmı tarafından güçlü bir şekilde desteklenebilir: Örneğin, son anketler, ankete katılan birçok Amerikalı'nın "önyargılı veya yanlış" raporlar yayınlayan haber kuruluşlarının kapatılmasını onaylayacaklarını gösterdiğini gösteriyor.¹³

Elbette, bu tür yargıları kimin yapacağı belli değil: Bazı raporlar tamamen uydurma olsa da, daha geniş anlamda taraflı veya yanlış olan şey genellikle bakanın gözündedir. Gazeteler genellikle isimsiz kaynaklara güvenirlir ve bu nedenle belirli bir raporun geçerli olduğunu kanıtlayamazlar. Bu standarda göre, bir icra organı *Washington Post*'un Watergate hikayelerini yayınlama hakkını pekala reddetmiş olabilir; Beyaz Saray'a göre bunlar uydurmaydı. Örneğin, Rus yayın ağı RT'nin 2016 seçimlerinden önce yaptığı şeylerin çoğu, yalnızca Breitbart Haber Ağı'nda veya diğer sağ alt ABD haber kuruluşlarında görünen hikayeleri vurgulamaktı.

Açıkça "sahte" haberlerin yayınlanmasını engellemeye yönelik çabalar, dezenformasyon noktasının çoğunu gözden geçiriyor. Propagandacılar, düpedüz uydurmalara kapılmanın tehlikelerini anlarlar ve çoğu zaman bunlardan yeterince kolayca kaçınabilirler. Nitelikli dezenformasyon uzmanları, şüpheli gerçeklerden ve yarı gerçeklerden oluşan bir kar fırtınasını, yanıltıcı olabilecek daha büyük bir anlatıda bir araya getiriyor, ancak her zaman gerçeklere dayanmıyor.

¹³ Flemming Rose ve Jacob Mchangama, "Tarih Kanıtlıyor Hükümetin Sahte Haberleri Düzenlemesinin Ne Kadar Tehlikeli Olduğunu" *Washington Post*, 3 Ekim 2017.

yanlış iddialar Nihai zorluk, meşru ve “gayrimeşru” konuşma arasında ayrım yapmanın zorluğudur.

Bu sorunlar ve sanal toplumsal savaşın yarattığı artan tehdit, ifade özgürlüğünün doğası ve sınırları hakkında yeni bir diyalog kurmamızı gerektiriyor. Aslında, kabul etmek istesek de istemesek de buna zaten sahibiz: Facebook veya Twitter gibi platformlar, belirli türdeki ırkçı veya taciz edici gönderilerin kaldırılması gerektiği konusunda hemfikir olduklarında, bunun yerine açıkça örtük bir denge standardı vardır. tüm konuşmalara izin verilmesi gereken mutlaklıyetçi bir duruş. Ama buradaki yokuşlar çok kaygan. Peki ya sağcı milliyetçi bakış açıları: İzin verilmeli mi? Öyleyse, neden nefret dolu, şiddeti teşvik eden aşırılık yanlısı mesajlar olmasın? Bu soruları çözmek, ifade özgürlüğünün karakteri ve sınırları hakkında şimdiye kadar denenmiş en dikkatli ve incelikli tartışmalardan bazılarını gerektirecektir.

Bir Yanıt Tasarlamak: İlk Gündem

Bu tür uzun vadeli tartışmalar sürerken, ABD ve diğer demokrasilerin bu tehditlere karşı dayanıklılıklarını güçlendirmek için atabilecekleri birkaç adım var. En büyük zorluk, ABD hükümeti içinde bu tür tehditlere verilecek yanıtın nasıl organize edileceğini belirlemektir. “Bilgi ortamı güvenliği” için bariz bir yuva yoktur. Kurumsal yapılar sorunu bu analizin kapsamı dışındadır, ancak bu risklerin azaltılmasına yardımcı olabilecek önemli reformlarla birlikte ele alınmalıdır. Bu reformlardan bazıları aşağıdaki bölümlerde özetlenmiştir.

Araştırmaya ve Anlamaya Yatırım Yapın

Bu çalışma için yaptığımız konuşmaların ve analizlerin çoğunda tutarlı bir tema, gelişen bilgi küresinin gerçek karakteri, olası yönleri, bu süreçteki temel nedensel dinamikler, popülasyonların çeşitli sosyal yaşam biçimlerine nasıl tepki verdiği de dahil olmak üzere farkındalığımızın sınırları olmuştur. manipülasyon ve en etkili cevapların neler olabileceği. Esnek bir bilgi küresinin ve sağlam bir sosyal topografyanın temel özellikleri nelerdir? Bu hedeflere ulaşp ulaşmadığımızı değerlendirmek için hangi ölçütleri kullanabiliriz?

Demokratik hükümetler, sosyal medya şirketleri ve gelişmiş toplumlarda enformasyonun rolüne derinden bağlı olan diğer şirketler ve vakıflar, bu tür araştırmaları kavramsallaştırmaya, finanse etmeye, teşvik etmeye ve bu tür araştırmalara yardım etmeye yönelik yatırımlarını iki katına çıkarmalıdır, bulguları bir kişi için rahatsız edici olsa bile. yönetim veya iş modeline özel yaklaşım.

Bu süreçte, araştırmacıların artık gizli tutulan birçok veri tabanına, algoritmaya ve bilgi depolama ve akışının diğer temel mekanizmalarına daha iyi erişime ihtiyaçları olacaktır. Bilgi dünyasının temel unsurlarına hakim olan sosyal medya platformları tarafından kullanılan özel modelleri büyük ölçüde aklımızda tutuyoruz. Şirketlerin bu tür bilgilerin kontrolünü sürdürmekte kazanılmış bir menfaati olması anlaşılabilir bir durumdur. Ancak ifşa etmeme anlaşmaları gibi uygun kontrollerle, tehdit ve risk kaynaklarını daha iyi anlamak için araştırmacılara yeterince “kitaplarını açabilirler”.

Bilgiye Dayalı Sosyal Manipülasyonun En Kötü Biçimlerine Karşı Aşılama ve Dayanıklılık Biçimleri Oluşturmaya Başlayın

Kampanyalar, kendilerini dışarıdan gelen taleplere oluştuktan sonra karşı koymakla sınırlamamalı, aynı zamanda bu tür iddialara ve kampanyalara karşı direnç oluşturmak için önceden adımlar atmalıdır. Önceden uyarı, yerleşik anlatıların sonradan ele alınmasından daha etkili olabilir. ¹⁴ Bir çalışma, halkı iklim değişikliğiyle ilgili yanlış bilgilere karşı aşılamanın yollarını inceledi. Güvenilir bilimsel fikir birliği mesajlarının, yanlış bilgilerle baltalandığında etkinliklerini kaybettiğini buldu. Ancak fikir birliği bir aşılama biçimi olarak sunulduğunda, sonraki yanlış bilgilere karşı dirençli kalabilir. ¹⁵

Toplumsal aşılama yönündeki çabalar, halkların direncini artırmak için halk ve medya eğitimini içerebilir - veya bir kaynağın öne sürdüğü gibi, "Amerikan nüfusu genelinde analitik becerileri sistematik olarak yeniden inşa edin ve bunu sağlamak için medyaya yatırım yapın.

¹⁴ Paul ve Matthews, 2016, s. 9–10.

¹⁵ Sander van der Linden, Anthony Leiserowitz, Seth Rosenthal ve Edward Maibach, “İklim Değişikliği Hakkında Yanlış Bilgiye Karşı Halkı Aşılama”, *Küresel Zorluklar*, Cilt. 1, Sayı 2, 2017.

tıklamalar değil, gerçekler tarafından yönlendirilir.”¹⁶ Ukrayna ve Finlandiya hükümetleri, eleştirel düşünme ve bilgi tüketimi programlarını bir ölçüde başarıyla denediler; küresel demokrasiler, deneyleri ortaya çıktıkça en iyi uygulamaları paylaşabilir. Büyük ölçekli halk eğitiminin etkinliği şüpheyeye açık olmaya devam ediyor, ancak IREX'in “Ayırt Etmeyi Öğren” programı gibi umut verici anekdot örnekleri var ve hedef nüfusun dezenformasyonu ayırt etme yeteneğinde ölçülebilir gelişmeler elde etti.¹⁷

Bu hedefin peşinden giderken, demokratik hükümetler, demokratik bir bilgi-kürenin “beyaz kan hücreleri” rolünü oynayabilecek bir dizi özel kuruluşa ilham vermeye, fon sağlamaya ve desteklemeye başlayabilir. Bu savunma hattı, yurttaş sosyal bilimcilerin yüzlerce deney yapması ve fikirleri bilemek için sonuçlar üzerinde çalışmasıyla, sosyal manipülasyon kampanyalarına yanıt vermeye yönelik deneme yanılma girişimlerini temsil edecektir. Çevrimiçi radikal mesajlarla mücadele çabalarından bir ders, genel olarak hükümetlerin ve özel olarak ABD hükümetinin bu tür kampanyalarda çok az güvenilirliğe sahip olmasıdır. Çaba, çevrimiçi ortamda daha güvenilir bağımsız aktörler etrafında toplanmalıdır. Bu nedenle Amerika Birleşik Devletleri'nin, sosyal medyadaki etkili aktörleri karşı dezenformasyon mesajları üretmeleri için güçlendirmek ve desteklemek için tasarlanmış kendi “etkileyiciler kampanyasına” ihtiyacı var.¹⁸

Bu kampanyanın bir kısmı izleme ve değerlendirmeye ayrılabilir: Dezenformasyon akışları, doğru bilgilerden farklı kalıplar izler. Nispeten az sayıda site tarafından hızlı ve yoğun bir şekilde abartılacak, oysa tipik geçerli haberler daha kademeli bir viral model izliyor. Bu nedenle, bu tür kampanyalar için belirteçler geliştirmek, yanlış bilgileri tespit etmek ve potansiyel olarak ömrünün başlarında buna karşı koymak mümkündür. İlişkilendirme araştırması geliyor; Facebook'un Rus botlarını takip etme yöntemi genel bir yeteneğe dönüştürülmeli ve daha geniş bir alana yayılmalıdır.

Diğer dağıtılmış çabalar, gerçekleri kontrol etmeye veya bir konudaki dezenformasyonla mücadele için bir “hızlı müdahale ekibi” sağlamaya ayrılabilir.

¹⁶ Nina Jankowicz, “Rusya'nın Bilgi Savaşına Karşı Savunmanın Tek Yolu,” *Yeni York Times*, 25 Eylül 2017.

¹⁷ Bu program hakkında bilgi için bkz. IREX, *Ayırt Etmeyi Öğrenin (L2D)—Medya Okuryazarlığı Eğitim*, tarihsiz.

¹⁸ Helmus ve Bodine-Baron, 2017, s. 2-3.

anbean bazında. Bu tür dağıtılmış çabalar, kaynağın güvenilirliğine ve okuyucuya iddianın geçerliliği hakkında anında bir fikir veren diğer niteliklere dayalı hikayeleri etiketlemeye odaklanabilir. Bu sınıflandırma her zaman işe yaramayacaktır: Özellikle, kendi kendini tanımlayan belirli yankı odaları söz konusu olduğunda, bu tür güvenilirlik raporları bir fark yaratmayabilir ve hatta ters etki yapabilir. Bununla birlikte, çoğu bilgi tüketicisi için, bir raporun güvenilir olup olmayacağına dair bir fikir vermeye yardımcı olabilirler.

Bugün Sosyal Medyanın Oynadığı Öncü Rolü ve Bu Alanda Yürütülen Bilgi Kontrolü Tartışmalarının Çoğunun Emsal Belirleyen Karakterini Ciddiye Alın

Hükümetler, sosyal medya platformlarını sorunları mümkün olan en üst düzeyde çözmeye teşvik edebilecek eylemlere giderek daha fazla bakmalıdır. Bu süreçte hükümetler, platformların sorunu çözmek için önümüzdeki iki ila üç yıl içinde yapabilecekleri dört ila beş şeyi belirlemeli.

Birçok sosyal medya şirketi, risklerin gerektirdiğinden daha yavaş olsa da, bu yönde hareket etmeye başlıyor. Face-book, bu haberi yayımlayan veya yayınlayan kuruluş için Wikipedia sitesine bağlanacak haber akışı bağlantılarına bir düğme ekliyor. Buradaki fikir, kullanıcılara kaynağın güvenilirliğini hızlı bir şekilde anlama yeteneği vermektir.¹⁹ Facebook ayrıca, yanlış bilgi olabilecek makaleleri tespit etmek için bir dizi dışarıdan bilgi kontrol kuruluşu kurmuştur. Üretilmiş bilgileri algılamak için belirli tetik tellerine çarpan makalelerin sistematik olarak derecesini düşürecek algoritma revizyonlarını düşündü - ancak daha sonra testler orantısız bir şekilde muhafazakar bölgelere çarpacağını gösterdiğinde geri çekildi. Daha sonra hem kullanıcı odaklı hem de algoritmik yanıtları denedi (bunları tanımlamak için anahtar kelimeler ve ifadeler kullanarak), sonunda ikincisine karar verdi, çünkü

¹⁹ Josh Constone, "Facebook, Bağlantılarda Yayıncı Bilgi Düğmesi ile Sahte Haberlerle Mücadele Etmeye Çalışıyor," *TechCrunch*, 5 Ekim 2017.

pratikte daha iyi performans gösterdi ve çünkü insan haber küratörlerinin siyasi önyargıları hakkında endişeler dile getirildi. 20

Amerikalıların Olayları Anlamlandırmasına Yardımcı Olabilecek Yeni, Genel Olarak Güvenilir Bilgi Aracı Kurumlar Kurmak İçin Tasarlanan Yatırımlar Yapın

Hükümetler (özel vakıflar ve aktivistler gibi), internet tarayıcıları (özellikle yeni yaklaşımlarda öncülük etmeye istekli olanlar) gibi bilgi şirketleri arasında, gözden geçirilmiş algoritmalar, yeni tarayıcı uzantıları, yeni tarayıcı uzantıları, ve neyin işe yaradığını görmek için farklı siteleri ve kaynakları derecelendirin ve sıralayın. Amaç, hükümet politikası tarafından aranan genel aşılama etkisine katkıda bulunacak sinyaller göndermek olacaktır. Günümüzün zorluklarından biri, halkın gördüklerinin doğru olup olmadığına dair bir fikir edinmek için güvenilebileceği saygın ve güvenilir aracı kaynakların azalmasıdır. Temel doğrulama kuruluşlarının yanı sıra, farklı türde revize edilmiş aracı kurumlarla deneyler yapmak, sanal toplumsal saldırganlığın etkisini azaltmaya yardımcı olabilir.

Böyle bir düşüncenin bir örneği, nasıl çalıştıklarını ve hükümetin (veya hayırsever veya analitik kuruluşların) onları nasıl güçlendirebileceğini veya bilgi akışını şekillendirmek için yenilerini nasıl inşa edebileceğini daha iyi anlamak için sosyal medya ağlarındaki etkileyicilerin rolünü araştırmak olabilir. Yakın tarihli araştırmaların bir bulgusu, sosyal ağlardaki etkili merkezlerin, hangi bilgilerin hangi insanlara ulaştığı konusunda orantısız bir sorumluluğa sahip olmasıdır. Bu tür etkileyiciler, dezenformasyondan ziyade doğruluk kaynakları olmaya ikna edilebildikleri ölçüde, ağ çağı için yeni bir tür aracı bilgi kurumu haline gelebilirler.

20 Josh Constine, "Facebook Sahte Haberlerle Sadece Kullanıcı Raporlarıyla Değil, Yapay Zekayla Savaşmayı Seçti," *TechCrunch*, 14 Kasım 2016.

Sanal Toplumsal Saldırganlığın Kullanımını Kısıtlayan Uluslararası Normlara Yönelik Çalışmaya Başlayın

Sanal toplumsal savaşın en büyük riski, 1945'ten beri büyük ölçüde hüküm süren ve ülkeler arasında barışın korunmasına yardımcı olan toprak bütünlüğü normunun sinsi, kademeli bir bozulmasını temsil etmesi olabilir. Uluslar birbirlerine sanal ama son derece zarar verici yollarla saldırmaya başladıkları ölçüde, bölgesel saldırmazlık konusundaki mevcut fikir birliği çökebilir ve sonunda büyük ölçekli silahlı maceracılığa yol açabilir. Diğer saldırganlık biçimlerinde olduğu gibi, caydırıcılık savunmaya güçlü bir şekilde katkıda bulunabilir, ancak ülkelerin statü ve prestijini temel ilkelere saygı göstermelerine yardımcı olan uluslararası normlar da aynı şekilde katkıda bulunabilir.

Potansiyel sanal çatışmalarda önde gelen katılımcıların çoğu şu anda bu tür resmi normları kabul edecek durumda değil. Bu kısmen, Amerika Birleşik Devletleri, Çin ve Rusya arasındaki artan rekabet güvensizliğinden ve hatta (bilgi güvenliği alanında) Avrupa Birliği'nin ABD'nin bu meselelere yaklaşımına olan inanç eksikliğinden dolayı doğrudur. Kısmen doğrudur, çünkü yolun etkili kurallarını hecelemek için bu zorluklar hakkında henüz yeterince bilgi sahibi değiliz. Bununla birlikte, Amerika Birleşik Devletleri en az iki başlangıç adımı atabilir: (1) bu tür normlara olan ilgisini açıkça ortaya koymak ve (2) böyle bir normatif mimarinin nasıl görünebileceğine ilişkin akademik tartışmalara fon sağlamaya ve aktif olarak katılmaya başlamak.

Başta Yapay Zeka Destekli Bilgi Kanalları, Sanal ve Artırılmış Gerçeklik ve Algoritmik Karar Verme olmak üzere Gelişen Teknolojilerin Çalışmalarını ve Güvenlik Açıklarını Daha İyi Anlayın

Amerika Birleşik Devletleri ve diğer demokrasiler dikkatli olmazsa, bu teknolojilerin özel uygulamasındaki ilerlemeler, politika ve hatta anlayışın önüne geçecek ve demokratik toplumlar için yoğun kırılğanlıklar yaratacaktır. Sanal toplumsal savaşın tehlikeleri ve demokratik toplumların ve gelişmiş ekonomilerin bu tür bilgi uygulamalarına belirgin şekilde artan bağımlılığı, bunların potansiyel etkileri ve demokrasilerin kendilerini korumak için atabilecekleri adımlar hakkında araştırma yapılması gerektiğine işaret ediyor.

Bu kategoriler muhtemelen demokrasilerin kendilerini
yanıt zırhlamaları için gerekli olan

türlerin yalnızca geniş bir taslağını temsil eder.

sanal toplumsal savaşın potansiyel tehdidine karşı, en azından bilgisel yönleri açısından. Ortaya çıkan bu saldırganlık biçimleri, daha önce görülmemiş bir ulusal güvenlik tehdidi olan ileri demokrasiler için önemli bir tehlikeyi temsil ediyor. Özellikle nükleer çağda ve doğrudan bölgesel saldırganlığa karşı genel bir küresel uzlaşmanın hüküm sürdüğü bir çağda, büyük ölçekli istilalar çoğunlukla geçmişte kaldı.

Ancak ordular caydırılabilirken, bilgi dünyasının ve ulusların daha geniş sosyal topografyasının kademeli, düşük seviyeli düşmanca manipülasyonu saldırganlığın yeni sınırı olabilir. Beşinci, Altıncı ve Yedinci Bölümlerde özetlenen gelecekler, ortaya çıkan teknolojilerin ve tekniklerin, sanal toplumsal savaş *potansiyelinin* neredeyse kesinlikle ortaya çıkmakta olduğu anlamına geldiğini kuvvetle göstermektedir. Bugün tek soru, demokrasilerin bu tehdide karşı kendilerini kontrol etmek ve savunmak için bir araya gelip gelmeyecekleri. Bu son bölümde özetlenen kategoriler, her ikisini de yapmak için bir başlangıç gündeminin bir parçasını temsil eder.

Referanslar

Adamic, Lada ve Natalie Glance, “The Political Blogosphere and the 2004 US Election: Divided They Blog”, Weblogging Ecosystem üzerine İkinci Yıllık Çalıştayda sunulan makale, Chiba, Japonya: Association for Computing Machinery, 2005.

Adler, Simon, “Son Dakika Haberleri,” *Radiolab* , 27 Temmuz 2017. 23 Ocak 2019 itibariyle:

<http://www.radiolab.org/story/breaking-news/>

Adobe Inc., “#VoCo. Adobe MAX 2016 (Sneak Peeks),” 4 Kasım 2016. Şu tarihten itibaren

23 Ocak 2019:

<https://www.youtube.com/watch?v=I3l4XLZ59iw>

Aharanov, Alex, “Artırılmış ve Sanal Gerçekliğin Geleceği Nedir?” *Jabil Blog* , 27 Mart 2018. 5 Mart 2019 itibariyle:

<https://www.jabil.com/insights/blog-main/future-of-augmented-and-virtual-reality-technology.html>

Ahluwalia, Rohini, “İkna Direncine Dayanan Psikolojik Süreçlerin İncelenmesi” , *Tüketici Araştırmaları Dergisi* , Cilt. 27, No. 2, 2000, s. 217–232.

Allen, Greg ve Taniel Chan, *Yapay Zeka ve Ulusal Güvenlik* , Cambridge, Mass.: Belfer Bilim ve Uluslararası İlişkiler Merkezi, Harvard Kennedy Okulu, Temmuz 2017.

Allenby, Braden R., “Silahlaştırılmış Anlatı Çağı veya Nereye Gittiniz Walter Cronkite?” *Bilim ve Teknoloji Sorunları* , Cilt. 33, Sayı 4, Yaz 2017.

Allport, Gordon, “Attitudes”, Carl Murchison, ed., *A Handbook of Social Psikoloji* , Worcester, Mass.: Clark University Press, 1935.

Anand, Bharat N., “ABD Medyasının Sorunları Sahte Haberlerden Çok Daha Büyük

and Filter Bubbles,” *Harvard Business Review* , 5 Ocak 2017. 20 Ocak itibariyle, 2019:

<https://hbr.org/2017/01/>

biz-medya-sorunlari-sahte-haber-ve-filtre-kabarciklarindan-cok-daha-buyuktur

Andrasik, Andrew J., *İnsanları Hacklemek: Sanal ile Gelişen Paradigma Reality*, SANS Enstitüsü, Bilgi Güvenliği Okuma Odası, Kasım 2017. As 22 Ocak 2019:

<https://www.sans.org/reading-room/whitepapers/testing/hack-insan-gelisten-paradigma-sanal-gerceklik-38180>

Arquilla, John ve David Ronfeldt, *The Emergence of Noopolitik: Toward an Amerikan Bilgi Stratejisi*, Santa Monica, California: RAND Corporation, MR-1033-OSD, 1999. 1 Mart 2019 itibarıyla:

https://www.rand.org/pubs/monograph_reports/MR1033.html

Arsene, Codrin, “Yakında Dünyamızda 8 Şekilde Devrim Yaratacak IoT Fikirleri,” *Y Media Labs*, 24 Kasım 2016. 22 Ocak 2019 itibarıyla:

<https://ymedialabs.com/internet-of-things-ideas/>

Auletta, Ken, “How the Math Men Overthrew the Mad Men,” *New Yorker*, 21 Mayıs 2018. 20 Ocak 2019 itibarıyla:

<https://www.newyorker.com/news/annals-of-communications/matematik-erkekler-deli-adamlari-nasil-devirdi>

Bakshy, Eytan, Jake M. Hofman, Winter A. Mason ve Duncan J. Watts, “Everyone's an Influencer: Quantifying Influence on Twitter,” *Fourth ACM Uluslararası Web Arama ve Veri Madenciliği Konferansı, Konferans Bildirileri*, Hong Kong: Bilgisayar Makineleri Derneği, 2011, s. 65-74.

Bakshy, Eytan, Solomon Messing ve Lada Adamic, “Possure to Ideologically Diverse News and Opinion on Facebook,” *Science*, Cilt. 348, No. 6239, 2015, s. 1130-1132.

Barabási, Albert-László, *Linked: Her Şey Başka Her Şeye Nasıl Bağlanır? ve İş, Bilim ve Günlük Yaşam için Ne Anlama Geliyor*, New York: Temel Kitaplar, 2014.

Bennett, W. Lance ve Shanto Iyengar, “A New Era of Minimal Effects? Siyasal İletişimin Değişen Temelleri,” *Journal of Communication*, Cilt. 58, No. 4, 2008, s. 707-731.

Berger, Jonah, *Contagious: Why Things Catch On*, New York: Simon ve Schuster, 2013.

Bialik, Kristen ve Katerina Eva Matsa, “Key Trends in Social and Digital News Media,” *Pew Research Center*, 4 Ekim 2017. 20 Ocak 2019 itibarıyla: <http://www.pewresearch.org/fact-tank/2017/10/04/sosyal-ve-dijital-haber-medyasinda-temel-trendler/>

Biocca, Frank, “İzleyicilerin Siyasal Mesajların Zihinsel Modelleri: Televizyonun Semantik İşleme Teorisine Doğru”, Frank Biocca, ed., *Television and Siyasal Reklam*, Cilt. I: *Psikolojik Süreçler*, Hillsdale, NJ: Lawrence Erlbaum Ortakları, 1991.

Bjørnskov, Christian ve Stefan Voigt, “Anayasal Ayrıntı ve Sosyal Güven,” *Public Choice* , Cilt. 161, No. 1/2, 2014, s. 91–112.

“Blockchain ve Nesnelerin İnterneti: IoT Blockchain Fırsatı and Challenge,” *i-SCOOP* , Eylül 2016 (Şubat 2018’de güncellendi). itibariyle 22 Ocak 2019:

<https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/>

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam DI Kramer, Cameron Marlow, Jaime E. Settle ve James H. Fowler, “A 61-Million-Person Experiment in Social Influence and Political Mobilization,” *Doğa* , Cilt. 489, 2012, s. 295–298.

Boxell, Levi, Matthew Gentzkow ve Jesse M. Shapiro, “Daha Fazla İnternet Kullanımı, ABD Demografik Grupları Arasındaki Politik Kutuplaşmanın Daha Hızlı Büyümesiyle İlişkili Değil”, *Proceedings of the National Academy of Sciences* , Cilt. 114, No. 40, Ekim 2017a, s. 10612–10617.

———, “Medya Amerikalıları Ayırıyor mu?” *New York Times* , 6 Aralık, 2017b. 24 Ocak 2019 itibariyle:

<https://www.nytimes.com/2017/12/06/opinion/is-media-driving-americans-apart.html>

Boyd, Clark, “Konuşma Tanıma Teknolojisinin Dünü, Bugünü ve Geleceği” *Başlangıç* , 10 Ocak 2018. 22 Ocak 2019 itibariyle:

<https://medium.com/swlh/konusma-tanima-teknoloji-cf13c179aaf-gecmiş-şimdi-ve-geleceği>

Boyd, Danah, “Your Data Is Manipulated,” *Data and Society: Points* , 4 Ekim 2017. 23 Ocak 2019 itibariyle: <https://points.datasociety.net/your-data-is-being-manipulated-a7e31a83577b>

———, “Algoritmik Çözümizm Retoriğinin Ötesinde,” *Veri ve Toplum: Puanlar* , 11 Ocak 2018. 23 Ocak 2019 itibariyle:

<https://points.datasociety.net/algoritmik-çözümçülüğün-retoriğinin-ötesinde-8e0f9cdada53>

Brennan, Jason, “Trump, Seçmenler Kelimenin Tam anlamıyla Cahil Olduğu İçin Kazandı,” *Yabancı*

Politika , 10 Kasım 2016. 24 Ocak 2019 itibariyle:

<https://foreignpolicy.com/2016/11/10/apartların-dansı-trump-clinton-seçim-cumhuriyetçi-demokrat/>

Brewster, Signe, “Bir Haftayı Chatbotlarla Yaşayarak Harcadım—Bütün Bu Kendi Kendine Yardım Edin mi?” *Kablolu* , 4 Ocak 2018.

Brown, Ian, “Bir Siber Sürpriz Hayal Etmek: Çin Güveni Hedeflemek için Çalınan OPM Kayıtlarını Nasıl Kullanabilir?” *War on the Rocks* , 22 Mayıs 2018. 20 Ocak 2019 itibariyle: <https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-hedef-güven/>

Bulger, Monica ve Patrick Davison, *The Promises, Challenges and Futures of Medya Okuryazarlığı* , New York: Veri ve Toplum Araştırma Enstitüsü, Şubat 2018.

As

20 Ocak 2019:

https://datasociety.net/pubs/oh/DataAndSociety_Media_Literacy_2018.pdf

Cai, Haoye, Chunyan Bai, Yu-Wing Tai ve Chi-Keung Tang, “Derin Video İnsan Eylem Dizilerinin Oluşturulması, Öngörülmesi ve Tamamlanması,” *Avrupa*

Computer Vision 2018, Conference Proceedings , Münih, Almanya,

Eylül 2018. 4 Mart 2019 itibariyle:

<https://arxiv.org/pdf/1711.08682.pdf>

Campbell, Troy ve Justin Friesen, “Neden İnsanlar 'Gerçeklerden Uçarlar’,” *Scientific Amerikan* , 3 Mart 2015. 20 Ocak 2019 itibariyle:

<https://www.scientificamerican.com/article/why-people-fly-from-facts/>

Cardenal, Juan Pablo, Jacek Kucharczyk, Grigoriy Meseznikov ve Gabriela Pleschová, *Sharp Power: Rising Authoritarian Influence* , Washington, DC: National Endowment for Democracy, Aralık 2017.

Carey, John M., Brendan Nyhan, Benjamin Valentino ve Mingnan Liu, “Gerçeklerin Şişirilmiş Görünümü? Tercihler ve Eğilimler, Deflategate Skandalı Hakkında Komplo İnançlarını Nasıl Şekillendiriyor,” *Research and Politics* , Cilt. 3, Sayı 3, Temmuz–Eylül 2016, s. 1–9.

Casey, Michael J. ve Paul Vigna, “In Blockchain We Trust,” *MIT Technology İnceleme* , 9 Nisan 2018.

Castells, Manuel, *Ağ Topluluğunun Yükselişi* , New York: Wiley-Blackwell, 2009.

Chan, Man-pui Sally, Christopher R. Jones, Kathleen Hall Jamieson ve Dolores Albarracín, “Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation,” *Psychological Science* , Cilt. 28, No. 11, 2017, s. 1531–1546.

Cheng, Justin, Lada Adamic, P. Alex Dow, Jon Michael Kleinberg ve Jure Leskovec, “Cascades Tahmin Edilebilir mi?” *Yirmi Üçüncü Uluslararası Dünya Geniş Ağ Konferansı, Konferans Bildirileri* , Seul: Hesaplama Derneği Makine, 2014, s. 925–936.

Can Public içinde “Hesaplamalı Propagandanın Arkasındaki Psikolojiyi Anlamak” Diplomasi İnternette Hayatta Kalmak mı? Washington, DC: ABD Danışma Komisyonu Kamu Diplomasisi, 2017a, s. 19–24.

———, *The MADCOM Future* , Washington, DC: Atlantik Konseyi, 2017b.

Cialdini, Robert, *Ön Suasion: Etkilemenin ve İkna Etmenin Devrimci Bir Yolu* , Yeni York: Simon ve Schuster, 2016.

Clarke, Richard A., *Siber Savaş: Ulusal Güvenliğe Bir Sonraki Tehdit ve Ne Yapmalı*

Bunu Yap , New York: Ecco, 2010.

Cobb, Michael D., Brendan Nyhan ve Jason Reifler, “İnançlar Her Zaman Sebat Etmez: Onlar Hakkında Olumlu Bilgiler Gözden Geçirildiğinde Politik Figürler Nasıl Cezalandırılır,” *Politik Psikoloji*, Cilt. 34, No. 3, Haziran 2013, s. 307–326.

Constine, Josh, “Facebook Sahte Haberlerle Sadece Kullanıcı Raporlarıyla Değil, Yapay Zekayla Savaşmayı Seçti,” *TechCrunch*, 14 Kasım 2016.

———, “Facebook, Bağlantılardaki Yayıncı Bilgi Düğmesiyle Sahte Haberlerle Mücadele Etmeye Çalışıyor,” *TechCrunch*, 5 Ekim 2017.

Cook, John, Ullrich KH Ecker ve Stephan Lewandowsky, “Yanlış Bilgi ve Nasıl Düzeltilir”, Robert Scott ve Stephan Kosslyn, ed., *Gelişen Trends in the Social and Behavioral Sciences*, New York: John Wiley and Sons, 2015.

———, “Yanlış Bilgiyi Aşılama Yoluyla Nötralize Etmek: Yanıltıcı Argümantasyon Tekniklerini Ortaya Çıkarmak Etkilerini Azaltır,” *PLOS One*, Cilt. 12, Sayı 5, 2017, sayfa 1-21.

Cummings, ML, Heather M. Roff, Kenneth Cukier, Jacob Parakilas ve Hannah Bryce, *Yapay Zeka ve Uluslararası İlişkiler: Bozulma Beklenen*, Londra: Chatham House, 2018.

Cutsinger, Paul, “Mark Cuban: Ses, Ortam Bilişimi Gelecektir. Geliştiriciler Hemen Girmeli,” *Amazon Alexa Blog*, 25 Mart 2019. Şu andan itibaren

19 Nisan 2019:

<https://developer.amazon.com/blogs/alexa/post/0902e3c5-9649-47e5-b705-984666b85125/mark-cuban-voice-ambient-computing-are-the-the-the-ve-neden-gelistiriciler-simdi-olmal>

DeMers, Jayson, “Çevrimiçi Pazarlamayı Daha İyi İçin Şekillendiren 7 Yeni Teknoloji (Umarız),” *Forbes*, 15 Ağustos 2016. 22 Ocak 2019 itibarıyla: <https://www.forbes.com/sites/jaysondemers/2016/08/15/7-yeni-teknolojiler-skekillendirme-cevrimi-ci-pazarlama-daha-iyi-biz-umariz/#4d8173761fd6>

Devlin, Hannah, “İnsan-Robot Etkileşimleri 'Duygusal' Chatbot ile İleriye Adım Atıyor,” *The Guardian*, 5 Mayıs 2017. 23 Ocak 2019 itibarıyla:

<https://www.theguardian.com/technology/2017/may/05/insan-robot-etkilesimleri-duygusal-sohbet-makine-sohbet-robotu-ile-adim-adim-adim>

Diaz, Jesus, “CGI'nın Garip, Vahşi Geleceği,” *Fast Company*, 19 Ekim 2017. 23 Ocak 2019 itibarıyla:

<https://www.fastcodesign.com/90147151/what-lies-beyond-the-uncanny-valley>

Druckman, James, “Çerçeveleme Etkilerinin Sınırları Üzerine: Kim Çerçeveleyebilir?” *günlük Siyaset*, Cilt. 63, No. 4, 2001, s. 1041–1066.

Duggan, Maeve ve Aaron Smith, “Sosyal Medyada Siyasi Çevre”, *Pew Araştırma Merkezi*, 25 Ekim 2016.

Eagly, Alice H. ve Shelly Chaiken, “İletişimci Özelliklerinin Fikir Değişikliği Üzerindeki Etkisinin Bir Nitelik Analizi: İletişimci Çekicilik Örneği”, *Journal of Personality and Social Psychology* , Cilt. 32, No. 1, 1975, s. 136–144.

Edwards, George C., III, *Sağır Kulaklarda: Zorba Minberin Sınırları* , New Haven, Bağlantı: Yale University Press, 2006.

Edwards, Kari ve Edward E. Smith, “Argümanların Değerlendirilmesinde Bir Doğrulama Önyargısı”, *Journal of Personality and Social Psychology* , Cilt. 71, No. 1, 1996, s. 5-24.

Engber, Daniel, “LOL Something Matters,” *Slate* , 3 Ocak 2018.

Epley, Nicholas ve Thomas Gilovich, “Motivated Reasoning'in Mekaniği”, *Journal of Economic Perspectives* , Cilt. 30, No. 3, 2016, s. 133–140.

Evans, Gareth, “Robotik Böcekler, 'Duvarda Uçan' Gözetlemeye Yepyeni Bir Anlam Katıyor,” *Army Technology* , 16 Mart 2015. 23 Ocak 2019 itibarıyla: <https://www.army-technology.com/ozellikler/ozellikrobotik-böcekler-add-tamamen-yeni-anlam-duvarda-uçmak-gözetim-4531866/>

“Eye in the Sky,” *Radiolab* , 18 Haziran 2015. 23 Ocak 2019 itibarıyla: <http://www.radiolab.org/story/eye-sky/>

“Sahte Haber: Henüz Hiçbir Şey Görmediniz,” *The Economist* , 1 Temmuz 2017.

22 Ocak 2019:

<https://www.economist.com/news/science-and-technology/21724370-generating-inandırıcı-ses-ve-video-sahte-olaylar-sahte-haber-siz-görmediniz>

Farrell, Henry, “American Democracy Is a Easy Target,” *Foreign Policy* , 17 Ocak 2018. 23 Ocak 2019 itibarıyla:

<http://foreignpolicy.com/2018/01/17/american-democracy-was-asking- onun için/>

Fazio, Lisa K., Nadia M. Brashier, B. Keith Payne ve Elizabeth J. Marsh, “Bilgi, Hayali Gerçeğe Karşı Korumaz,” *Journal of Experimental Psikoloji* , Cilt. 144, No. 5, 2015, s. 993–1002.

Ferran, Lee, “Derin Sahte Haber'in Yaklaşan Krizine Dikkat Edin” *RealClearLife* ,

27 Temmuz 2018. 23 Ocak 2019 itibarıyla:

<http://www.realclearlife.com/technology/yalancılar-temettü-dikkat-the-the-the-deep-of-deep-sahte-news/#1>

Flaxman, Seth, Sharad Goel ve Justin M. Rao, “Filter Bubbles, Echo Chambers ve Online News Consumption,” *Public Opinion Quarterly* , Cilt 80, Sayı. S1, 2016, s. 298–320.

Fleming, Jennifer, “Medya Okuryazarlığı, Haber Okuryazarlığı veya Haber Takdir? Stony Brook Üniversitesi'nde Haber Okuryazarlığı Programına İlişkin Bir Vaka Çalışması,” *Gazetecilik ve Kitle İletişim Eğitimsi* , Cilt. 69, No. 2, 2014, s. 146–165.

Fletcher, Richard, Alessio Cornia, Lucas Graves ve Rasmus Kleis Nielsen, *Avrupa'da "Sahte Haber" ve Çevrimiçi Dezenformasyonun Erişimini Ölçmek*, Oxford, Birleşik Krallık: Reuters Gazetecilik Araştırmaları Enstitüsü, Oxford Üniversitesi, Şubat 2018.

Flynn, DJ, Brendan Nyhan ve Jason Reifler, "Yanlış Algıların Doğası ve Kökenleri: Siyaset Hakkında Yanlış ve Desteklenmeyen İnançları Anlamak," *Politik Psikoloji*, Cilt. 38, Ek. 1, 2017, s. 127–150.

Fukuyama, Francis, *Güven: Sosyal Erdemler ve Refahın Yaratılışı*, Yeni York: Özgür Basın, 1995.

Gal, David ve Derek D. Rucker, "Şüphedeyken Bağırın! Şüphenin Proselize Etme Üzerindeki Paradoksal Etkileri," *Psikoloji Bilimi*, Cilt. 21, No. 11, 2010, s. 1701-1707.

Gallup, *Derinlemesine: Konular A'dan Z'ye: Kurumlara Güven*, 2018. 24 Ocak itibarıyla,

2019:

<https://news.gallup.com/poll/1597/confidence-institutions.aspx>

Gans, John A., Jr., "Governing Fantasyland", *Hayatta Kalma*, Cilt. 60, Sayı 3, Haziran-Temmuz 2018, s. 195–202.

Garrett, R. Kelly, "Echo Chambers Online?: İnternet Haber Kullanıcıları Arasında Politik Motivasyonlu Seçici Maruz Kalma", *Journal of Computer-Mediated İletişim*, Cilt. 14, No. 2, 2009a, s. 265–285.

———, "Politik Olarak Motive Edici Güçlendirme Arayışı: Seçici Maruz Kalma Tartışmasını Yeniden Çerçevelemek", *Journal of Communication*, Cilt. 59, No. 4, 2009b, s. 676–699.

Garrett, R. Kelly, Dustin Carnahan ve Emily K. Lynch, "Kaçınmaya Doğru Bir Dönüş mü? Selective Exposure to Online Political Information, 2004–2008," *Politik Davranış*, Cilt. 35, No. 1, 2013, s. 113–134.

Garrett, R. Kelly ve Paul Resnick, "İnternetteki Politik Parçalanmaya Karşı Direnmek," *Daedalus*, Cilt. 140, No. 4, Güz 2011, s. 108–120.

Gentzkow, Matthew ve Jesse M. Shapiro, "İdeolojik Ayrım Çevrimiçi ve Çevrimdışı," *Quarterly Journal of Economics*, Cilt. 126, No. 4, 2011, s. 1799–1839.

Gholipour, Bahar, "Yeni Yapay Zeka Teknolojisi Her Sesi Taklit Edebilir", *Scientific American*,

2 Mayıs 2017. 23 Ocak 2019 itibarıyla:

<https://www.scientificamerican.com/article/new-ai-tech-can-mimic-any-voice/>

Giddens, Anthony, *The Consequences of Modernity*, Cambridge, Birleşik Krallık: Polije, 1990.

Glanville, Jennifer L., Matthew A. Andersson ve Pamela Paxton, "Sosyal Bağlantılar Güven Yaratır mı? Yeni Boylamsal Verileri Kullanan Bir İnceleme," *Sosyal Kuvvetler*, Cilt. 92, No. 2, 2013, s. 545–562.

Glanville, Jennifer L. ve Pamela Paxton, “Güvenmeyi Nasıl Öğreniriz? Genelleştirilmiş Güven Kaynaklarının Doğrulayıcı Bir Dörtlü Analizi”, *Sosyal Psikoloji Aylık* , Cilt. 70, No. 3, 2007, s. 230–242.

Yazılım ve Toplumun Geleceğine İlişkin Küresel Gündem Konseyi, *Deep Shift: Teknolojide Devrilme Noktaları ve Sosyal Etki* , Köln, İsviçre: Dünya Ekonomik Forum, 2015.

Gorman, Jack ve Sara Gorman, *Mezarı İnkâr Etmek: Neden Gerçekleri Görmezden Geliyoruz?*

Bu Bizi Kurtaracak , New York: Oxford University Press, 2016.

Grassegger, Hannes ve Mikael Krogerus, “Weaken from Within,” *New Republic* , 2 Kasım 2017.

Grieco, Elizabeth, “Daha Fazla Amerikalı Haber İçin Birden Fazla Sosyal Medya Sitesine Dönüyor,” *Pew Araştırma Merkezi* , 2 Kasım 2017. 20 Ocak 2019 itibarıyla: <http://www.pewresearch.org/fact-tank/2017/11/02/daha-fazla-amerikalı-haber-için-çoklu-sosyal-medya-sitelerine-dönüyor/>

Grigonis, Hillary, “AI, İnsanların Bilgisayar Tarafından Oluşturulan En Gerçekçi Görüntülerinden Bazılarını Oluşturuyor,” *Digital Trends* , 30 Ekim 2017. 23 Ocak 2019 itibarıyla: <https://www.digitaltrends.com/computing/nvidia-araştırma-bilgisayar- tarafından- oluşturulan- görüntüler/>

Guess, Andrew M., *Medya Seçimi ve Denetleme: Çevrimiçi İzlemeden Kanıtlar Veri* , iş piyasası raporu, New York: New York Üniversitesi, 6 Eylül 2016. As 15 Kasım 2017:

<https://www.scribd.com/document/323356298/>

Medya-Seçim-ve-Denetleme-Çevrimiçi-İzleme-Verilerinden-Kanıt-

Guyer, Joshua J. ve Leandre R. Fabrigar, “Attitudes and Behavior,” James Wright, ed., *International Encyclopedia of the Social & Behavioral Sciences* , Cilt. II, 2. baskı, New York: Elsevier, 2015.

Haidt, Jonathan, “Yirmi Birinci Yüzyıl İçin Ahlakî Psikoloji”, *Journal of Ahlak Eğitimi* , Cilt. 42, No. 3, 2013, s. 281–297.

Harari, Yuval Noah, “Big Data, Google and the End of Free Will,”

Financial Times , 26 Ağustos 2016. 23 Ocak 2019 itibarıyla:

<https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>

Harwell, Drew, “Şirketler Yeni Ödül Kazanan Bir Para Birimi: Vücut

Ölçümlerimiz”, *Washington Post* , 16 Ocak 2018. 23 Ocak 2019 itibarıyla:

https://www.washingtonpost.com/business/economy/companies-yeni-ödüllü-para-birimi-vücutumuz-ölçümleri-to-toplamak-için-yarış/2018/01/16/5af28d98-f6e8-11e7-beb6-c8d48830c54d_story.html

Cennet, Douglas, “Dr. Bot Seni Şimdi Görecek,” *MIT Technology Review* , Kasım/Aralık 2018.

Heffernan, Virginia, “Hackerların Alacakaranlığı”, *Wired* , Şubat 2018.

- Helmus, Todd C. ve Elizabeth Bodine-Baron, "İŞİD Muhaliflerini Güçlendirmek Twitter'da," Santa Monica, Kaliforniya: RAND Corporation, PE-227-RC, 2017. 4 Mart 2019:
<https://www.rand.org/pubs/perspectives/PE227.html>
- Heritage Foundation, "Derin Sahteler: Mahremiyet, Demokrasi, and National Security," panel tartışması, Washington, DC, 19 Temmuz 2018. 23 Ocak 2019:
<https://www.heritage.org/homeland-security/event/derin-sahte-belirgin-meydan-okuma-gizlilik-demokrasi-ve-ulusal-guvenlik>
- Higginbotham, Stacey, "IBM, Nesnelerin İnternetini Fethetmek için Watson'ı Getiriyor," *Fortune* , 15 Aralık 2015. 20 Ocak 2019 itibarıyla:
<http://fortune.com/2015/12/15/ibm-watson-iot/>
- Holley, Peter, "Gezicilerdeki Büyük Birader: Araba Şirketiniz Neden Biliyor Olabilir? Eşinizden Daha Çok Hakkınızda," *Washington Post* , 15 Ocak 2018. İtibarıyla 23 Ocak 2019:
<https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-neden-arabanizin-sirketi-sizin-hakkinizda-esinizden-daha-fazlasini-biliyor-olabilir/>
- Horowitz, Michael C., "Yapay Zeka, Uluslararası Rekabet ve Güç Dengesi," *Texas National Security Review* , Cilt. 1, Sayı 3, Mayıs 2018, s. 36–57.
- Hosanagar, Kartik ve Vivian Jair, "Algoritmalarla Şeffaflığa İhtiyacımız Var, Ama Çok Fazlası Geri Tepebilir" *Harvard Business Review* , 25 Temmuz 2018.
- Huang, Jian, Henriëtte Maassen van den Brink ve Wim Groot, "Kolej Eğitimi ve Sosyal Güven: Nedensel Mekanizmalar Üzerine Kanıta Dayalı Bir Çalışma," *Sosyal Göstergeler Araştırması* , Cilt. 104, No. 2, 2011, s. 287–310.
- Huang, Zheping, "Çin Polisi Yüzleri Tanıyabilen Güneş Gözlüğü Takıyor," *Defence One* , 9 Şubat 2018.
- Hvistendahl, Mara, "Inside China's Wst New Experiment in Social Ranking," *Wired* , 14 Aralık 2017.
- Hwang, Tim, *Manevra ve Manipülasyon: Online'ın Askeri Stratejisi Üzerine Bilgi Savaşı* , Carlisle Kışlası, Pa.: Stratejik Araştırmalar Enstitüsü, 2019.
- "İnsanların Konuşma Kalıplarını Taklit Etmek Sorun Getirebilir " *Economist* , 20 Nisan 2017. 23 Ocak 2019 itibarıyla:
<https://www.economist.com/news/science-and-technology/21721128-you-took-words-right-out-my-mouth-imitating-peoples-speech-patterns>
- Inglehart, Ronald ve Pippa Norris, *Trump, Brexit ve Popülizmin Yükselişi: Ekonomik Olmayanlar ve Kültürel Tepki* , fakülte araştırma çalışma kağıdı, Cambridge, Mass.: Harvard Kennedy Okulu, RWP16-026, Ağustos 2016.

The Digital Universe of Opportunities'de "Yönetici Özeti: Veri Büyümesi, İş Fırsatları ve BT Zorunlulukları" : Zengin Veri ve Nesnelerin İnternetinin Artan Değeri , Framingham, Mass., Nisan 2014.

IREX, *Fark Etmeyi Öğrenin (L2D)—Medya Okuryazarlığı Eğitimi* , tarihsiz. itibariyle

23 Ocak 2019:

<https://www.irex.org/project/learn-discern-l2d-media-literacy-training>

Isenberg, Daniel J., “Grup Kutuplaşması: Eleştirel Bir İnceleme ve Meta-Analiz,” *Kişilik ve Sosyal Psikoloji Dergisi* , Cilt. 50, No. 6, 1986, s. 1141–1151.

İsmail, Kaya, “AI ve Algoritmalar: Fark Nedir?” *CMS Tel* , 26 Ekim, 2018. 20 Ocak 2019 itibariyle:

<https://www.cmswire.com/information-management/ai-vs-algoritmalar-fark-nedir/>

Iyengar, Shanto, Guarav Sood ve Yphtach Lelkes, “Affect, Not Ideology: A Social Identity Perspective on Polarization,” *Public Opinion Quarterly* , Cilt. 76, No. 3, 2012, s. 405–431.

J. Walter Thompson Intelligence, *Speak Easy* , New York, Haziran 2017. 22 Ocak 2019:

<https://www.jwtintelligence.com/trend-reports/speak-easy-global-edition/>

Jain, Shailendra Pratap ve Steven S. Posavac, “Ön Satın Alma Özelliği Doğrulanabilirliği, Kaynak Güvenilirliği ve İkna,” *Tüketici Psikolojisi Dergisi* , Cilt. 11, No. 3, 2001, s. 169–180.

Jankowicz, Nina, “Rusya'nın Bilgi Savaşına Karşı Savunmanın Tek Yolu,” *New York Times* , 25 Eylül 2017. 23 Ocak 2019 itibariyle: <https://www.nytimes.com/2017/09/25/opinion/the-only-way-to-defend-against-russias-information-war.html>

Jarvis, Brooke, "Yaşamak O'nu Nasıl Yeneceğimdi", *Wired* , Aralık 2017.

Joseph, Regina, “Geleceğe Bakış: Influence's New Masters tarafından Gizli Bir Devrim”, Weston Aviles ve Sarah Canna'da, ed. , *Etki Üzerine Beyaz Kitap Yükselen Bağlılık Çağı* , Washington, DC: ABD Savunma Bakanlığı, Ağustos 2017.

Jowett, Garth S. ve Victoria O'Donnell, *Propaganda and Persuasion* , 3. baskı, Thousand Oaks, Calif.: SAGE Publications, 1999.

Judis, John B., *Popülist Patlama* , New York: Columbia Global Reports, 2016.

Kaplan, Jonas T., Sarah I. Gimbel ve Sam Harris, “Kişinin Siyasi İnançlarını Karşı Kanıt Karşısında Sürdürmenin Sinirsel İlişkileri,” *Scientific Raporlar* , Cilt. 6, Madde 39589, 2016.

Karras, Tero, Timo Aila, Samuli Laine ve Jaakko Lehtinen, "Geliştirilmiş Kalite, Kararlılık ve Varyasyon için GAN'ların Aşamalı Büyümesi", *Altıncı Uluslararası Öğrenme Temsilleri Konferansı, Konferans Bildirileri*, Vancouver, Kanada, 2018.

Kavanagh, Jennifer ve Michael D. Rich, *Truth Decay: An İlk Keşif Amerikan Kamu Hayatında Gerçeklerin ve Analizlerin Azalan Rolü*, Santa Monica, Kaliforniya: RAND Corporation, RR-2314-RC, 2018. 4 Mart 2019 itibariyle: https://www.rand.org/pubs/research_reports/RR2314.html

Kelman, Herbert C., "Tutumlar Canlı ve İyidir ve Eylem Alanında Kazançla İstihdam Edilir," *Amerikan Psikolog*, Cilt. 29, No. 5, 1974, s. 310-324.

Kilovaty, Ido, "Doxfare: Politik Olarak Motive Edilen Sızıntılar ve Silahlaştırılmış Bilgi Çağında Müdahale Dışı Normunun Geleceği," *Harvard National Güvenlik Dergisi*, Cilt. 9, No. 1, 2018, s. 146-179.

Knack, Stephen ve Philip Keefer, "Sosyal Sermayenin Ekonomik Bir Getirisi Var mı? Ülkeler Arası Bir Soruşturma," *Quarterly Journal of Economics*, Cilt. 112, No. 4, 1997, s. 1251-1288.

Knight, Will, "Yapay Zekanın Kalbinde Karanlık Sır", *MIT Technology Review*, 11 Nisan 2017. 22 Ocak 2019 itibariyle: <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>

———, "ABD Ordusu Deepfakes ve Diğer Yapay Zeka Hilelerini Yakalama Çabalarını Finanse Ediyor," *MIT Technology Review*, 23 Mayıs 2018a.

———, "Bu Yapay Zeka Programı Sizi Bir Tartışmada Yenebilir—Ama Değil Ne Dediyini Bilin," *MIT Technology Review*, 19 Haziran 2018b. Ocak ayı itibariyle 22, 2019:

<https://www.technologyreview.com/s/611487/this-ai-program-could-beat-you-in-a-argument-ai-ne-ne-söylediyini-bilmiyor/>

———, "Eğlence ve Sabotaj Amaçlı Araştırma Robotları Kaçırılabilir", *MIT Technology Review*, 24 Temmuz 2018c.

———, "Savunma Bakanlığı Derin Sahteleri Yakalamak İçin İlk Araçları Üretti," *MIT Technology Review*, 7 Ağustos 2018d.

———, "Bu İnanılmaz Gerçekçi Sahte Yüzler, Algoritmaların Artık Bize Nasıl Bulaşabileceğini Gösteriyor," *MIT Technology Review*, 14 Aralık 2018e.

Kolbert, Elizabeth, "Neden Gerçekler Fikirlerimizi Değiştirmiyor," *New Yorker*, 27 Şubat 2017. 20 Ocak 2019 itibariyle: <https://www.newyorker.com/magazine/2017/02/27/neden-gerçekler-fikirlerimizi-değiştirme>

- Kozinets, Robert, “Sosyal Medya İnsanların Tutkularını Nasıl Ateşliyor? Extremist Divisions,” *The Conversation*, 13 Kasım 2017. 20 Ocak itibarıyla, 2019:
<http://theconversation.com/nasil-sosyal-medya-insanlar-tutkular-ve-inşa-aşırılık-bölümleri-86909>
- Kravetz, Lee Daniel, *Garip Bulaşma*, New York: HarperCollins, 2017.
- Kunda, Ziva, “Motive Reasoning Davası”, *Psikolojik Bülten*, Cilt. 108, No. 3, Kasım 1990, s. 480-498.
- Lakoff, George, “Beynin Metafor Devresinin Haritalandırılması: Gündelik Akılda Metaforik Düşünce,” *Frontiers in Human Neuroscience*, Cilt. 8, Madde 958, 2014.
- Langston, Jennifer, “Lip-Syncing Obama: New Tools Turn Audio Clips to Realistic Video,” *UW News*, 11 Temmuz 2017. 23 Ocak 2019 itibarıyla: <http://www.washington.edu/news/2017/07/11/dudak-senkronizasyon-obama-yeni-araclar-ses-kliplerini-gerçekçi-videoya-dönüştür/>
- Lau, Richard R., David J. Andersen, Tessa M. Ditonto, Mona S. Kleinberg ve David P. Redlawsk, “Effect of Media Environment Diversity and Advertising Tone on Information Search, Selective Exposure, and Affective Polarization,” *Politik Davranış*, Cilt. 39, No. 1, 2017, s. 231–255.
- LaZarsfeld, Paul, Bernard Berelson ve Hazel Gaudet, *Halkın Seçimi: Nasıl Seçmen Bir Başkanlık Kampanyasında Kararını Veriyor*, New York: Duell, Sloan, ve Pearce, 1948.
- Lelkes, Yphtach, Guarav Sood ve Shanto Iyengar, “Düşman Kitle: Geniş Bant İnternete Erişimin Partizan Etkisi Üzerindeki Etkisi,” *American Journal of Siyaset Bilimi*, Cilt. 61, No. 1, 2017, s. 5–20.
- Letki, Natalia, “Sivil Ahlakın Kökenlerini Araştırmak: Güven, Sosyal Sermaye ve Kurumsal Performans,” *Politik Davranış*, Cilt. 28, No. 4, 2006, s. 305–325.
- “Deneysel Olalım: Adobe MAX Sneaks’in Arkasında,” *Adobe Blog*, 4 Kasım 2016. 22 Ocak 2019 itibarıyla: <https://theblog.adobe.com/lets-get-experimental-behind-the-adobe-max-gizlice-girer/>
- Leviathan, Yaniv, “Google Duplex: An AI System for Real-World Tasks Over the Phone”, *Google AI Blog*, 8 Mayıs 2018. 22 Ocak 2019 itibarıyla: <https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html>
- Lewandowsky, Stephan, Ullrich KH Ecker ve John Cook, “Yanlış Bilginin Ötesinde: 'Hakikat Sonrası' Çağı Anlamak ve Başa Çıkmak”, *Journal Applied Research in Memory and Cognition*, Cilt. 6, Sayı 4, Aralık 2017, s. 353-369.

Lewandowsky, Stephan, Ullrich KH Ecker, Colleen M. Seifert, Norbert Schwarz ve John Cook, “Yanlış Bilgi ve Düzeltmesi: Devam Eden Etki ve Başarılı Önyargılardan Kurtulma,” *Psikolojik Bilimin Kamu Yararına* , Cilt. 13, No. 3, 2012, s. 106–131.

Li, Yitong, Martin Renqiang Min, Dinghan Shen, David Carlson ve Lawrence Carin, “Metinden Video Üretimi,” *Otuz İkinci AAAI Yapay Yapay Zeka Konferansı Intelligence, Conference Proceedings* , New Orleans, La.: Association for the Yapay Zekanın Gelişimi, Şubat 2018.

Lin, Herbert ve Jackie Kerr, *Siber Destekli Bilgi/Etki Savaşı Üzerine ve Manipülasyon* , çalışma kağıdı, Stanford, California: Stanford Center for Uluslararası Güvenlik ve İşbirliği, 13 Ağustos 2017. 19 Nisan 2019 itibariyle: <https://cisac.fsi.stanford.edu/publication/siber-etkin-bilgi-etki-savas-ve-manipulasyon>

Lord, Charles G., Lee D. Ross ve Mark R. Lepper, “Önyargılı Asimilasyon ve Tutum Kutuplaşması: Önceki Teorilerin Daha Sonra Düşünülen Kanıt Üzerindeki Etkileri,” *Kişilik ve Sosyal Psikoloji Dergisi* , Cilt. 37, No. 11, 1979, s. 2098–2109.

Lyrebird, “Büyük İnovasyonla Büyük Sorumluluk Gelir”, tarihsiz. itibariyle 12 Aralık 2017: <https://lyrebird.ai/ethics>

Magids, Scott, Alan Zorfas ve Daniel Leemon, “The New Science of Customer Emotions,” *Harvard Business Review* , Kasım 2015. 23 Ocak 2019 itibariyle: <https://hbr.org/2015/11/the-new-müşteri-duyguları-bilimi>

Maio, Gregory R. ve Geoffrey Haddock, *Tutum ve Tutum Psikolojisi Change* , Thousand Oaks, California: SAGE Publications, 2009.

Manjoo, Farhad, “Tech's 'Frightful 5' Öngörülebilir Gelecek için Dijital Yaşama Hakim Olacak,” *New York Times* , 20 Ocak 2016. 20 Ocak 2019 itibariyle: <https://www.nytimes.com/2016/01/21/teknoloji/teknoloji-korkutucu-5-hakim-olacak-dijital-yaşam-for-öngörülebilir-gelecek.html>

Martin, Gregory J. ve Ali Yörükoğlu, “Bias in Cable News: Persuasion and Polarization,” *American Economic Review* , Cilt. 107, No. 9, 2017, s. 2565–2599.

Matsa, Katarina Eva ve Elisa Shearer, “Sosyal Medya Platformlarında Haber Kullanımı 2018,” *Pew Araştırma Merkezi* , 10 Eylül 2018. 20 Ocak 2019 itibariyle: <http://www.journalism.org/2018/09/10/haber-kullanım-sosyal-medya-platformları-2018/>

Mazarr, Michael J., “Karamsarlık Sendromu,” *Washington Quarterly* , Cilt. 21, No. 3, 1998, s. 93–108.

Mercier, Hugo ve Dan Sperber, *The Enigma of Reason* , Cambridge, Mass.: Harvard Üniversitesi Yayınları, 2017.

Metz, Cade, “Nihayet, Aslında Çalışan Sinir Ağları,” *Wired* , 21 Nisan 2015.

Metz, Cade ve Keith Collins, “Bir Yapay Zeka 'Kedi-Fare Oyunu' Nasıl Üretilir?

Believable Fake Photos,” *New York Times* , 2 Ocak 2018. 23 Ocak itibariyle, 2019:

<https://www.nytimes.com/interactive/2018/01/02/technology/ai-generated-photos.html>

Meyer, Jared, “The Ignorant Voter,” *Forbes* , 27 Haziran 2016. 24 Ocak 2019 itibariyle: <https://www.forbes.com/sites/jaredmeyer/2016/06/27/amerikalı-seçmenler-cahildir-ama-apıal-değildir/#3d425e67ff17>

Mitzen, Jennifer, “Dünya Siyasetinde Ontolojik Güvenlik: Devlet Kimliği ve Güvenlik İkilemi,” *Avrupa Uluslararası İlişkiler Dergisi* , Cilt. 12, No. 3, 2006, s. 341–370.

Moore, James W., “Faillik Duygusu Nedir ve Neden Önemlidir?” *Psikolojide Sınırlar* , Cilt. 7, Madde 1272, Ağustos 2016.

Müller, Jan-Werner, *Popülizm Nedir?* Philadelphia, Pa.: Pennsylvania Üniversitesi Yayınları, 2016.

Munro, Geoffrey D. ve Peter H. Ditto, “Önyargılı Asimilasyon, Tutum Polarizasyonu ve Tepkilerde Stereotiple İlgili Bilimsel Bilgilere Etkisi”, *Kişilik ve Sosyal Psikoloji Bülteni* , Cilt. 23, No. 6, 1997, s. 636-653.

Mutz, Diana C. ve Paul S. Martin, “Siyasi Farklılıklar Arasında İletişimi Kolaylaştırma: Kitle İletişim Araçlarının Rolü”, *Amerikan Siyaset Bilimi İnceleme* , Cilt. 95, No. 1, 2001, s. 97-114.

Nagle, Angela, *Tüm Normları Öldür: 4chan ve Tumblr'dan Çevrimiçi Kültür Savaşları*

Trump ve Alt Sağ , Winchester, Birleşik Krallık: Sıfır Kitaplar, 2017.

Ulusal Halk Radyosu, “Güven ve Sonuçlar,” *TED Radyo Saati* , 15 Mayıs, 2015. 23 Ocak 2019 itibariyle:

<https://www.npr.org/programs/ted-radio-hour/406238794/trust-and-consequences>

———, “Büyük Veri Devrimi,” *TED Radyo Saati* , 9 Eylül 2016. 23 Ocak 2019:

<https://www.npr.org/programs/ted-radio-hour/492296605/big-data-revolution>

———, “5 Teknoloji Devi Nasıl Şirketlerden Çok Hükümetlere Benzer Oldu?” *Fresh Air* , 26 Ekim 2017. 20 Ocak 2019 itibariyle:

<https://www.npr.org/2017/10/26/560136311/5-teknoloji-devleri,şirketlerden-daha-çok-hükümetlere-nasıl-dönüştü?>

Neef, Dale, *Digital Exhaust* , Upper Saddle River, NJ: Pearson FT Press, 2014.

Newman, Eryn J., Mevagh Sanson, Emily K. Miller, Adele Quigley-McBride, Jeffrey L. Foster, Daniel M. Bernstein ve Maryanne Garry, “Adları Telaaffuzu Kolay Kişiler, İddiaların Doğruluğunu Destekliyor,” *PLOS One* , Cilt . 9, Sayı 2, 2014.

Ng, Alfred, “VR Systems Oculus Rift, HTC Vive Hacklere Karşı Savunmasız Olabilir,” *CNET* , 17 Nisan 2018.

Nicas, Jack, “YouTube İnsanları İnternetin En Karanlık Köşelerine Nasıl Çekiyor,” *Wall*

Street Journal , 7 Şubat 2018. 24 Ocak 2019 itibariyle:

[https://www.wsj.com/articles/](https://www.wsj.com/articles/youtube-izleyicileri-internets-darkest-corners'a-nasil-yonlendirir-1518020478)

youtube-izleyicileri-internets-darkest-corners'a nasıl yönlendirir-1518020478

Nichols, Tom, “Mezunlarımız Rubes,” *Chronicle of Higher Education* , 15 Ocak 2017a.

———, “Amerika Uzmanlığa İnancını Nasıl Kaybetti,”

Foreign Affairs , Mart–Nisan 2017b. 23 Ocak 2019 itibariyle:

[https://www.foreignaffairs.com/articles/united-states/2017-02-13/](https://www.foreignaffairs.com/articles/united-states/2017-02-13/nasil-amerika-kayip-inanç-uzmanlık) nasıl-amerika-kayıp-inanç-uzmanlık

Nie, Norman H., Darwin W. Miller III, Saar Golde, Daniel M. Butler ve Kenneth Winneg, “The World Wide Web and the US Political News Market,” *American Journal of Political Science* , Cilt. 54, No. 2, 2010, s. 428–439.

Nietzsche, Friedrich, *Hakikat ve Yalan Üzerine: Seçilmiş Yazılar* , çev. ve ed. Taylor Carman, New York: Harper Çok Yıllık, 2010.

Norveç Tüketici Konseyi, *#Toyfail: Tüketici ve Mahremiyetin Analizi İnternet Bağlantılı Üç Oyuncakta Sorunlar* , Oslo, Aralık 2016. 1 Mart itibarıyla, 2019:

<https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/>

Nyhan, Brendan ve Jason Reifler, “Düzeltilmeler Başarısız Olduğunda: Politik Yanlış Algıların Kalıcılığı,” *Politik Davranış* , Cilt. 32, No. 2, 2010, s. 303–330.

———, *Yanlış Bilgilendirme ve Doğrulama: Sosyal Bilimlerden Araştırma Bulguları* , Washington, DC: Yeni Amerika, Şubat 2012.

———, “Olaylar Hakkında Yanlış Bilgiyi Değiştirmek: Nedensel Düzeltilmelerin Deneyisel Testi,” *Deneyisel Siyaset Bilimi Dergisi* , Cilt. 2, No. 1, 2015a, s. 81–93.

———, “Grip Aşısı Hakkındaki Efsaneleri Düzeltmek İşe Yarar mı? Düzeltici Bilginin Etkilerinin Deneyisel Bir Değerlendirmesi,” *Vaccine* , Cilt. 33, No. 3, 2015b, s. 459–464.

———, “Gerçek Kontrolünün Seçkinler Üzerindeki Etkisi: ABD Eyalet Kanun koyucuları üzerinde bir Alan Deneyi,” *American Journal of Political Science* , Cilt. 59, No. 3, 2015c, s. 628–640.

———, “Yanlış Algıların Yaygınlığında Bilgi Açıkları ve Kimlik Tehdidinin Rolü”, *Seçimler, Kamuoyu ve Partiler Dergisi*, 2018, s. 1-23.

O’Neil, Cathy, *Weapons of Math Destruction: Büyük Veri Eşitsizliği Nasıl Artırıyor? ve Demokrasiyi Tehdit Ediyor*, New York: Broadway Books, 2016.

Osnos, Evan, “Making China Great Again”, *New Yorker*, 8 Ocak 2018.

Pardes, Arielle, “Kişisel Sohbet Botum Bana Yapay Zekanın Geleceği Hakkında Ne Öğretiyor”

Kablolu, 12 Kasım 2017. 22 Ocak 2019 itibarıyla:

[https://www.wired.com/story/](https://www.wired.com/story/benim-kisisel-sohbet-bot-replika-bana-yapay-zeka-hakkinda-ogrettikleri/)

benim-kisisel-sohbet-bot-replika-bana-yapay-zeka-hakkinda-ogrettikleri/

Pariser, Eli, *The Filter Bubble: İnternet Sizden Ne Saklıyor*, New York: Penguin Basını, 2011.

Pasquale, Frank, *Kara Kutu Derneği: Parayı Kontrol Eden Gizli Algoritmalar ve Bilgi*, Cambridge, Mass.: Harvard University Press, 2015.

Paul, Christopher ve Miriam Matthews, “Rus ‘Yanlışlık Yangın Hortumu’ Propaganda Modeli: Neden Çalışabilir ve Karşı Çıkmak İçin Seçenekler,” Santa Monica, California: RAND Corporation, PE-198-OSD, 2016. Mart itibarıyla 4, 2019: <https://www.rand.org/pubs/perspectives/PE198.html>

Pentland, Alex, *Sosyal Fizik: İyi Fikirler Nasıl Yayılır—Yeni Birinden Dersler Bilim*, New York: Penguin Press, 2014.

Perez, Sarah, “Ses Özellikli Akıllı Konuşmacıların 2022’ye Kadar ABD Hanelerinin %55’ine Ulaşmasını Sağladı, Diyor” *TechCrunch*, 8 Kasım 2017.

Persily, Nathaniel, “Demokrasi İnternette Hayatta Kalabilir mi?” *Demokrasi Dergisi*, Cilt. 28, Sayı 2, Nisan 2017.

Petty, Richard E., Russell H. Fazio ve Pablo Briñol, ed., *Attitudes: Insights from The New Implicit Measures*, New York: Psychology Press, 2008.

Pew Araştırma Merkezi, *Halkın Güncel Olaylara İlişkin Bilgisi Haberlerle Çok Az Değişti ve Bilgi Devrimleri*, Washington, DC, 15 Nisan 2007.

Phillips, Whitney, *Güzel Şeylere Sahip Olamamamızın Nedeni Bu: Çevrimiçi Trollük ve Ana Kültür Kültürü Arasındaki İlişki*, Cambridge, Mass.: MIT Yayınları, 2015.

Pierce, David, “Yeni Sanal Ofisinizin Keyfini Çıkarın,” *Wired*, Şubat 2018.

Pollard, Neal A., Adam Segal ve Matthew G. Devost, “Trust War: Dangerous Trends in Cyber Conflict,” *War on the Rocks*, 16 Ocak 2018. 23 Ocak itibarıyla, 2019:

<https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/>

Pratkanis, Anthony R. ve Elliot Aronson, *Age of Propaganda: The Everyday Use ve İnkarnın Kötüye Kullanılması*, New York: Henry Holt and Company, 2001.

Price, Rob, "AI ve CGI, Bilgi Savaşını Dönüştürecek, Sahtekarlıkları Artıracak ve Escalate Revenge Porn," *Business Insider* , 12 Ağustos 2017. 23 Ocak 2019 itibarıyla:

[http://www.businessinsider.com/](http://www.businessinsider.com/cgi-ai-sahte-video-ses-haber-aldatmaca-bilgi-savas-intikam-porno-2017-8)

[cgi-ai-sahte-video-ses-haber-aldatmaca-bilgi-savas-intikam-porno-2017-8](http://www.businessinsider.com/cgi-ai-sahte-video-ses-haber-aldatmaca-bilgi-savas-intikam-porno-2017-8)

Putnam, Robert, *Tek Başına Bowling: Amerikan Topluluğunun Çöküşü ve Canlanması* ,

New York: Simon ve Schuster, 2001.

Rabin-Havt, Ari, *Lies, Incorporated: The World of Post-Truth Politics* , New York: Çapa Kitapları, 2016.

Radinsky, Kira, "Algoritmalarınız Hackerlardan Korunmuyor," *Harvard Business İnceleme* , 5 Ocak 2016. 22 Ocak 2019 itibarıyla:

<https://hbr.org/2016/01/your-algorithms-are-not-safe-from-hackers>

Redlawsk, David P., "Sıcak Biliş mi, Soğuk Düşünce mi? Motive Edilmiş Akıl Yürütmenin Siyasi Karar Verme Üzerindeki Etkilerinin Test Edilmesi," *Journal of Politics* , Cilt. 64, No. 4, 2002, s. 1021–1044.

Redlawsk, David P., Andrew JW Civettini ve Karen M. Emmerson, "Duygusal Devrilme Noktası: Motive Edilmiş Akılcılar Hiç 'Anladım' mı?" *siyasi Psikoloji*, Cilt. 31, No. 4, 2010, s. 563–593.

Richardson, John H., "AI Sohbet Robotları, Bizi Öfkeliendirmeden Toplantı Planlamaya Çalışıyor," *Wired* , 24 Mayıs 2018. 22 Ocak 2019 itibarıyla:

<https://www.wired.com/story/xai-meeting-ai-sohbet-robotu/>

Robbins, Blaine G., "Kurumsal Kalite ve Genelleştirilmiş Güven: Tekrarlı Olmayan Nedensel Bir Model," *Sosyal Göstergeler Araştırması* , Cilt. 107, No. 2, 2012, s. 235–258.

Roberts, Graham, "Artırılmış Gerçeklik: Haberleri Evinize Nasıl Getireceğiz," *New York Times* , 1 Şubat 2018. 24 Ocak 2019 itibarıyla:

<https://www.nytimes.com/interactive/2018/02/01/spor/olimpiyatlar/nyt-ar-artirilmis-gerceklik-ul.html>

Rodriguez, Ashley, "Beş Yıl İçinde VR, ABD'de Netflix Kadar Büyük Olabilir" *Quartz* , 6 Haziran 2018. 22 Ocak 2019 itibarıyla:

[https://qz.com/1298512/](https://qz.com/1298512/vr-beş-yıllık-çalışma-şovlarında-netflix-in-the-bize-büyük-olabilir/)

[vr-beş yıllık-çalışma-şovlarında-netflix-in-the-bize-büyük-olabilir/](https://qz.com/1298512/vr-beş-yıllık-çalışma-şovlarında-netflix-in-the-bize-büyük-olabilir/)

Romano, Andrew, "Amerikalılar Ne Kadar Cahil?" *Newsweek* , 20 Mart 2011.

Roose, Kevin, "İşte Sahte Videolar da Geliyor," *New York Times* , 4 Mart,

2018. 23 Ocak 2019 itibarıyla:

<https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html>

Rose, Flemming ve Jacob Mchangama, "Tarih, Hükümetin Sahte Haberleri Düzenlemesini Sağlayın," *Washington Post* , 3 Ekim 2017.

23 Ocak 2019:

[https://www.washingtonpost.com/news/theworldpost/wp/2017/10/03/](https://www.washingtonpost.com/news/theworldpost/wp/2017/10/03/tarih-hükümete-sahip-olmanın-ne-kadar-tehlikeli-olduğunu-kanıtlıyor-düzenleme-sahte-haberler/)

[tarih-hükümete-sahip olmanın-ne-kadar-tehlikeli-olduğunu-kanıtlıyor-düzenleme-sahte-haberler/](https://www.washingtonpost.com/news/theworldpost/wp/2017/10/03/tarih-hükümete-sahip-olmanın-ne-kadar-tehlikeli-olduğunu-kanıtlıyor-düzenleme-sahte-haberler/)

Ross, Alec, *Geleceğin Endüstrileri* , New York: Simon ve Schuster, 2016.

Ross, Lee D., Mark R. Lepper, Fritz Strack ve Julia Steinmetz, “Sosyal Açıklama ve Sosyal Beklenti: Gerçek ve Varsayımsal Açıklamaların Öznel Olabilirlik Üzerindeki Etkileri,” *Kişilik ve Sosyal Dergisi Psikoloji* , Cilt. 35, No. 11, 1977, s. 817-829.

Rothman, Joshua, “Afterimage,” *New Yorker* , 12 Kasım 2018.

Rothstein, Bo ve Eric M. Uslaner, “Herkes İçin: Eşitlik, Yolsuzluk ve Sosyal Güven,” *World Politics* , Cilt. 58, No. 1, 2005, s. 41–72.

Rubin, Peter, “Sanal Gerçeklikte İşe Gideceksin,” *Wired* , Haziran 2018, s. 61.

Sabelman, Eric E. ve Roger Lam, “The Real-Life Dangers of Augmented Reality,” *IEEE Spectrum* , 23 Haziran 2015. 22 Ocak 2019 itibarıyla: [https://spectrum.ieee.org/consumer-electronics/ taşınabilir aletler/ gerçek-hayat-tehlikeleri-artırılmış-gerçeklik](https://spectrum.ieee.org/consumer-electronics/taşınabilir-aletler/gerçek-hayat-tehlikeleri-artırılmış-gerçeklik)

Sanger, David E., David D. Kirkpatrick ve Nicole Perlroth, “Dünya Bir Zamanlar Kuzey Kore Siber Gücüne Gülmüştü. No More,” *New York Times* , 15 Ekim, 2017. 23 Ocak 2019 itibarıyla: <https://www.nytimes.com/2017/10/15/world/asia/kuzey-kore-hacking-cyber-sony.html>

Scharre, Paul ve Michael C. Horowitz, *Yapay Zeka: Her Şey Politika Yapıcının Bilmesi Gerekenler* , Washington, DC: Yeni Bir Amerikalı Merkezi Güvenlik, Haziran 2018.

Schiff, Stacy, “The Interactive Truth,” *New York Times* , 15 Haziran 2005. 23 Ocak 2019: <https://www.nytimes.com/2005/06/15/opinion/the-interactive-truth.html>

Schneier, Bruce, *Herkesi Öldürmek İçin Buraya Tıklayın: Bir Hiper Sistemde Güvenlik ve Hayatta Kalma Bağlantılı Dünya* , New York: WW Norton, 2018.

Segal, Adam, *Hacked World Order: Uluslar Nasıl Savaşıyor, Ticaret, Manevra ve Dijital Çağda Manipülasyon* , New York: PublicAffairs, 2016.

Selk, Avi, "Bu Ses Klibi, Trump May Prelude A Future of Fake Human Voices", *Washington Post* , 3 Mayıs 2017. 22 Ocak 2019 itibarıyla: <https://www.washingtonpost.com/news/yenilikler/wp/2017/05/03/bu-koz-bir-robot-olarak-klip-insan-seslerinin-bir-gelecegi-baslangic-sesleri/>

Sen, Conor, “The 'Big Five', Tech Ecosystem'i Yok Edebilir,” *Bloomberg* , 15 Kasım 2017. 20 Ocak 2019 itibarıyla: <https://www.bloomberg.com/view/articles/2017-11-15/buyuk-beş-teknoloji-ekosistemini-yok-edebilir>

Shaikh, Faizan, “Üretici Düşman Ağlarına (GAN'lar) ve Vaatlerine Giriş Kılavuzu!” *Analytics Vidhya* , 15 Haziran 2017. 23 Ocak 2019 itibarıyla: <https://www.analyticsvidhya.com/blog/2017/06/ giris-uretici-dusman-aglari-gans/>

Shearer, Elisa ve Jeffrey Gottfried, “News Use Across Social Media Platforms 2017,” *Pew Research Center* , 7 Eylül 2017. 20 Ocak 2019 itibarıyla: <http://www.journalism.org/2017/09/07/ haber-kullanimi-sosyal-medya-platformlari-2017/>

Sherman, Justin ve Deb Crawford, “Securing America's Connected Infrastructure Can't Wait,” *War on the Rocks* , 4 Aralık 2018. 22 Ocak 2019 itibarıyla: <https://warontherocks.com/2018/12/ guvenli-amerika-bagli-altyapi-beklemez/>

Shields, David, *Reality Hunger: A Manifesto* , New York: Knopf, 2010.

Sides, John ve Jack Citrin, *Toplanmış Kitleler Ne Kadar Büyük? Nedenler ve Kamuoyunun Göçmen Popülasyonları Hakkındaki Yanlış Algılarının Sonuçları* , bildiri sunumu . Midwest Siyaset Bilimi Derneği'nin 65. Yıllık Ulusal Konferansı'nda, Chicago, 2007.

Silfversten, Erik, “Akıllı Bir Oyuncak Sadece Noel İçin Değil, Yaşam Boyu Kişisel Ayrıntılara Sahip Olabilir,” *RAND Blog* , Aralık 2017. 5 Mart 2019 itibarıyla: <https://www.rand.org/blog/2017/12/ a-akilli-oyuncak-olabilir-kisisel-ayrintilar-for-life-not.html>

Silhavy, Radek, Roman Senkerik, Zuzana Kominkova Oplatkova, Zdenka Prokopova ve Petr Silhavy, ed., *Intelligent Intelligence Trends in Intelligent Systems: Proceedings of the 6th Computer Science On-Line Conference 2017 (CSOC2017)* , Cilt. I, Cham, İsviçre: Springer International Publishing, 2017.

Skurnik, Ian, Carolyn Yoon, Denise C. Park ve Norbert Schwarz, “Yanlış İddialara İlişkin Uyarılar Nasıl Öneriler Oluyor,” *Tüketici Dergisi Araştırma* , Cilt. 31, No. 4, 2005, s. 713–724.

Sloman, Steven ve Philip Fernbach, *Bilgi Yanılsaması : Neden Asla Yalnız Düşün* , New York: Riverhead Books, 2017.

Smiley, Lauren, “Something To Watch Over Me,” *Wired* , Ocak 2018.

Soper, Taylor, “Çin'deki İnsanlar Neden Microsoft'un Xiaoice Virtual Companion ve Yapay Zeka Hakkında Ne Diyor?” , *GeekWire* , 25 Kasım 2015. 23 Ocak 2019 itibarıyla: <https://www.geekwire.com/2015/ insanlar-çin-aşk-microsofts-xiaoice-sanal-arkadaş-diyor-yapay-zeka/>

Spectre, Michael, *İnkarcılık: Mantıksız Düşünme Bilimsel İlerlemeyi Nasıl Engeller, Gezegeni Zarar Veriyor ve Hayatımızı Tehdit Ediyor* , New York: Penguin Press, 2009.

Stafford, Tom, “Psikoloji: Neden Kötü Haber Manşetlere Domined?” *BBC* , 29 Temmuz 2014. 20 Ocak 2019 itibarıyla:

<http://www.bbc.com/future/story/20140728-why-is-all-the-news-bad>

Stone, Peter, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe ve Astro Teller, *Yapay Zeka ve 2030'da Yaşam: Bir Yapay Zeka Üzerine Yüz Yıl Araştırması* , Stanford, Kaliforniya: Stanford Üniversitesi, Eylül 2016.

Strange, Adario, “Yüz İzleme Yazılımı, Herkesin Gerçek Zamanlı Olarak Her Şeyi Söylemesini Sağlıyor,” *Mashable* , 20 Mart 2016. 23 Ocak 2019 itibarıyla:

<http://mashable.com/2016/03/20/face-izleme-yazilimi/#U3o58PfQH8qI>

Stubbardsfield, Joseph M., Jamshid J. Tehrani ve Emma G. Flynn, "Seri Katiller, Örümcekler ve Siber Seks: Kentsel Efsanelerin Aktarılmasında Sosyal ve Hayatta Kalma Bilgisi Önyargısı", *İngiliz Psikoloji Dergisi* , Cilt. 106, No. 2, 2015, s. 288–307.

Suh, Chan S., Paul Y. Chang ve Yisook Lim, “Spill-Up and Spill-Over of Trust: An Extended Test of Cultural and Corporate Theories of Trust in South Korea,” *Sociological Forum* , Cilt. 27, No. 2, 2012, s. 504–526.

Sunstein, Cass R., *#Cumhuriyet: Sosyal Medya Çağında Bölünmüş Demokrasi* , Princeton, NJ: Princeton University Press, 2017.

Swift, Sanat, “Amerikalıların Kitle İletişim Araçlarına Güveni Yeni Bir Düşüşe Düşüyor,” *Gallup* , 14 Eylül 2016.

Taber, Charles S. ve Milton Lodge, “Siyasi İnançların Değerlendirilmesinde Motive Edilmiş Şüphencilik”, *Amerikan Siyaset Bilimi Dergisi* , Cilt. 50, No. 3, 2006, s. 755–769.

Tan, Chenhao, Vlad Niculae, Cristian Danescu-Niculescu-Mizil ve Lilian Lee, “Winning Arguments: Interaction Dynamics and Persuasion Strategies in Good-Faith Çevrimiçi Tartışmalar,” 25. *Uluslararası World Wide Web Konferansı, Konferans Bildirileri* , Montreal, Kanada: International World Wide Web Konferanslar Yönlendirme Komitesi, Nisan 2016, s. 613-624.

Taub, Amanda, “Sahte Haberin Gerçek Hikayesi Partizanlıktır,” *New York Times* , 11 Ocak 2017. 23 Ocak 2019 itibarıyla:

<https://www.nytimes.com/2017/01/11/upshot/the-real-story-about-fake-news-is-partisanship.html>

Thies, Jutus, Michael Zollhöfer, Marc Stamminger, Christian Theobalt ve Matthias Nießner, “Face2Face: Real-Time Face Capture and Reenactment of RGB Videos,” *IEEE Conference on Computer Vision and Pattern Recognition, Konferans Proceedings* , Las Vegas, Nev.: Elektrik ve Elektronik Mühendisleri Enstitüsü, 2016.

Thompson, Nicholas ve Fred Vogelstein, "Facebook's Two Years of Hell," *Wired* , Mart 2018.

Thorson, Emily, "İnanç Yankıları: Düzeltilmiş Yanlış Bilginin Kalıcı Etkileri", *Siyasi İletişim* , Cilt. 33, No. 3, 2016, s. 460–480.

Whysu, DK, *News as Entertainment: The Rise of Global Infotainment* , Londra: SAGE Yayınları, 2007.

Tiku, Nitasha, "Fotoğraflarımızı Paylaştığımız Kadar İsteyerek Duygusal Durumumuzu da Paylaşacağız," *Wired* , Haziran 2018.

Tormala, Zakary L. ve Richard E. Petty, "Beni Öldürmeyen Şey Beni Daha Güçlü Yapar: İknaya Karşı Direnmenin Tutum Kesinliği Üzerindeki Etkileri," *Journal of Kişisel ve Sosyal Psikoloji* , Cilt. 83, Sayı 6, 2002.

———, "Kaynak Güvenilirliği ve Tutum Kesinliği: İkna Direncinin Üst Bilişsel Analizi," *Tüketici Psikolojisi Dergisi* , Cilt. 14, No. 4, 2004, s. 427-442.

Tracy, Liz, "Microsoft'un Çinli Chatbot'u Xiaolce, Tay'ın aksine, Aslında Pleasant," *Ters* , 26 Mart 2016. 23 Ocak 2019 itibarıyla: <https://www.inverse.com/article/13387-microsoft-çin-sohbet-robotu>

Tucker, Patrick, "Strava's Sadece Başlangıç: ABD Ordusu Veri Sızıntısına Karşı Savaşı Kaybediyor," *Defense One* , 31 Ocak 2018.

ABD Savunma Bakanlığı, *Ortak Yayın 1-02: Savunma Bakanlığı Askeri ve İlişkili Terimler Sözlüğü* , Washington, DC, Kasım 2010.

Ullah, Haroon K., *Dijital Dünya Savaşı: İslamcılar, Aşırılıklar ve Siber Mücadele Üstünlük* , New Haven, Conn.: Yale University Press, 2017.

Amerika Birleşik Devletleri Yasası, Başlık 47, Bölüm 230, Saldırgan Materyalin Özel Engellenmesi ve Taranması için Koruma, 3 Ocak 2012.

Uslaner, Eric M., "Nerede Durduğunuz, Büyükanne ve Büyükbabanızın Nerede Oturduğuna Bağlıdır: Genelleştirilmiş Güvenin Kalıtılabilirliği," *Public Opinion Quarterly* , Cilt. 72, No. 4, 2008, s. 725–740.

van den Oord, Aäron, Tom Walters ve Trevor Strohman, "WaveNet Launches in the Google Assistant," *DeepMind Blog* , 4 Ekim 2017. 23 Ocak 2019 itibarıyla: <https://deepmind.com/blog/wavenet-launches -google-asistanı/>

van der Linden, Sander, Anthony Leiserowitz, Seth Rosenthal ve Edward Maibach, "İklim Değişikliği Hakkında Yanlış Bilgilendirmeye Karşı Halkı Aşlamak," *Global Challenges* , Cilt. 1, Sayı 2, 2017.

Vanian, Jonathan, "Facebook, Twitter, Sahte Haber ve Manipülasyonla Mücadelede Yeni Adımlar Atıyor," *Fortune* , 20 Ocak 2018. 24 Ocak 2019 itibarıyla: <http://fortune.com/2018/01/19/facebook-twitter -haber beslemesi-rusya-reklamları/>

Verghese, Abraham, “Teknoloji Doktorları Nasıl Büro İşçilerine Dönüştürülebilir?” *Yeni York Times Dergisi* , 16 Mayıs 2018.

Vettehen, PH ve M. Kleemans, “Açıkça Kanıtlamak? Duyumsallığın Haber Videosunda Harcanan Zamana Katkıları, *Electronic News* , Cilt. 12, No. 2, 2018, s. 113–127.

Vincent, James, “Yapay Zeka, Sahte Görüntü ve Video Yapmayı Hiç Olmadığı Kadar Kolaylaştıracak,” *The Verge* , 20 Aralık 2016. 23 Ocak 2019 itibarıyla: <https://www.theverge.com/2016/12/20/14022958/ai-goruntü-manipulasyon-olusturma-sahte-ses-video>

VivoText, ana sayfa, tarihsiz. 6 Mart 2019 itibarıyla: <https://www.vivotext.com/>

Vlahos, James, “Fighting Words,” *Wired* , Mart 2018.

Vosoughi, Soroush, Deb Roy ve Sinan Aral, “Çevrimiçi Doğru ve Yanlış Haberlerin Yayılması,” *Science* , Cilt. 359, No. 6380, 2018, s. 1146–1151.

Waltzman, Rand, “The Weaponization of Information: The Need for Cognitive Security”, Senato Silahlı Hizmetler Komitesi, Siber Güvenlik Alt Komitesi, Santa Monica, Kaliforniya: RAND Corporation, CT-473, 27 Nisan 2017. 5 Mart 2019: <https://www.rand.org/pubs/testimonies/CT473.html>

Weaver, Kimberlee, Stephen M. Garcia, Norbert Schwarz ve Dale T. Miller, “Bir Görüşün Popülerliğini Tanıdıklığından Çıkarsama: Tekrarlayan Bir Ses Bir Koro Gibi Seslendirebilir”, *Journal of Personality and Social Psychology* , Cilt. 92, No. 5, 2007, s. 821-833.

West, Darrell M., “Robotlar ve Yapay Zeka İşinizi Alacak mı? Ekonomik ve Otomasyonun Politik Sonuçları,” *Brookings Enstitüsü* , 18 Nisan 2018. 22 Ocak 2019: <https://www.brookings.edu/blog/techtank/2018/04/18/will-robots-and-ai-take-otomasyonun-is-ekonomik-ve-politik-sonuclari/>

Wharton, Bruce, Shawn Powers ve Markos Kounalakis, editörler, *Can Public Diplomacy Survive the Internet mi?* Washington, DC: ABD Kamu Diplomasisi Danışma Komisyonu, 2017, s. 7–11.

Whitson, Jennifer ve Adam Galinsky, “Kontrol Eksikliği Hayali Model Algısını Artırıyor,” *Science*, Cilt. 322, No. 5898, 2008, s. 115–117.

Witte, Kim, “Korkuyu Korku Temyizlerine Geri Döndürmek: Genişletilmiş Paralel Süreç Modeli,” *Communication Monographs* , Cilt. 59, No. 4, 1992, s. 329–349.

Witte, Kim ve Mike Allen, “Korku Temyizlerinin Meta-Analizleri: Etkili Halk Sağlığı Kampanyalarının Etkileri,” *Health Education and Behavior*, Cilt. 27, No. 5, 2000, s. 591–615.

Wittes, Benjamin ve Gabriella Blum, *Şiddetin Geleceği: Robotlar ve Mikroplar, Hackerlar ve Dronlar*, New York: Temel Kitaplar, 2015.

Wu, Hao-Yu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand ve William Freeman, “Eulerian Video Magnification for Revealing Subtle Changes in the World,” *ACM Transactions on Graphics*, Cilt. 31, No. 4, 2012, s. 1–8.

Wu, Tim, *Tüccarların Dikkatine: Kafamızın İçine Girmek İçin Destansı Karıştırma*, New York: Eski Kitaplar, 2016.

Yam, CY, “Derin Öğrenmeyi Kullanarak Metinden Duygu Algılama ve Tanıma,” *Microsoft Developer Blog*, 29 Kasım 2015. 22 Ocak 2019 itibarıyla: <https://www.microsoft.com/developerblog/2015/11/29/metinden-duygu-algilama-ve-tanima-kullanarak-derin-ogrenme/>

Yearsley, Liesl, “Yapay Zekanın İnsanları Manipüle Etme Gücü Hakkında Konuşmalıyız,” *MIT Technology Review*, 5 Haziran 2017. 22 Ocak 2019 itibarıyla: <https://www.technologyreview.com/s/608036/> İnsanları manipüle etmek için yapay zekanın-gücü hakkında-konuşmamız-ihtiyacımız var/

Siz, Jong-sung, “Sosyal Güven: Adillik Homojenlikten Daha Önemlidir,” *Politik Psikoloji*, Cilt. 33, No. 5, 2012, s. 701–721.

Yargıları İnsanlar Tarafından Yapılanlardan Daha Doğru” *Ulusal Bilimler Akademisi*, Cilt. 112, No. 4, 2015, s. 1036–1040.

Zhang, Han, Tao Xu, Hongsheng Li, Shaoting Zhang, Xiaogang Wang, Xiaolei Huang ve Dimitris Metaxas, “StackGAN: Yığılmış Üretken Düşman Ağlarla Metinden Foto-Gerçekçi Görüntü Sentezine,” *IEEE International Bilgisayarla Görme Konferansı, Konferans Bildirileri*, Venedik, İtalya: Institute of Elektrik ve Elektronik Mühendisleri, Ekim 2017.

Zmerli, Sonja ve Ken Newton, “Social Trust and Attitudes Toward Democracy,” *Public Opinion Quarterly*, Cilt. 72, No. 4, 2008, s. 706-724.

Gelişmiş bilgi ortamlarının evrimi, ekonomik ve sosyal sistemlerin etkin işleyişinin bilgi temellerini manipüle etme veya bozma çabalarını içeren yeni bir olası siber saldırganlık kategorisini hızla yaratıyor. RAND araştırmacıları bu büyüyen tehdide *sanal* özellikleri ve geleceğe yönelik etkilerinin bir analizinde *toplumsal savaş* . Sanal toplumsal savaş riskini anlamak için yazarlar, bu tekniklerin gelecekte nasıl gelişebileceğinin bazı ilk hatlarını çizmek için bir dizi kategorideki kanıtları araştırdılar. Değerlendirmeyi (1) Amerika Birleşik Devletleri ve diğer gelişmiş demokrasilerde bilgi ortamının değişen karakterindeki eğilimler üzerine ayrıntılı araştırmalara; (2) tutumlar ve inançlar üzerine sosyal bilim araştırmalarının içgörülerini; ve (3) düşmanca sosyal manipülasyon uygulamalarına ve onun daha ayrıntılı ve tehlikeli kuzeni sanal toplumsal savaşa dayanan ilgili yeni teknolojilerdeki gelişmeler. Yazarlar daha sonra sosyal manipülasyonun önümüzdeki on yılda gelişmiş toplumları nasıl etkileyebileceğine dair üç senaryo sunuyor. Analiz, ulusal güvenliğin giderek daha esnek bir bilgi ortamına ve güçlü bir sosyal topografyaya dayanacağı ve bu çatışmanın giderek ağlar arasında ve ağlar arasında sürdürüleceği dahil olmak üzere, ortaya çıkan sanal toplumsal savaş sorununu tanımlamaya yardımcı olabilecek bir dizi başlangıç özelliği önermektedir. Acilen daha fazla araştırmaya ihtiyaç duyulmasına rağmen, yazarlar, en kötü bilgi tabanlı sosyal manipülasyon biçimlerine karşı aşılama ve dayanıklılık biçimleri oluşturmak da dahil olmak üzere, bu artan risk karşısında demokratik direnci artırmak için birkaç ilk tepki yoluna işaret ederek sonuca varıyorlar. Gelişmekte olan teknolojilerin işleyişini ve güvenlik açıklarını daha iyi anlamak.



MİLLİ SAVUNMA ARAŞTIRMA ENSTİTÜSÜ

www.rand.org

30,00 \$

ISBN-10 1-9774-0272-0
ISBN-13 978-1-9774-0272-1

53000

