Bilgisayımsal
Propaganda
Araştırma Projesi

OXFORD
INTERNET
INSTITUTE

UNIVERSITY OF
OXFORD

Küresel Dezenformasyon Düzeni

2019 Organize Sosyal Medya Manipülasyonunun Küresel Dökümü

Samantha Bradshaw · Oxford Üniversitesi
Philip N. Howard · Oxford Üniversitesi

Rapor Özeti

Bilgisayımsal propaganda – toplumsal hayatı biçimlendirmek için algoritmaların, otomasyonun ve büyük verinin kullanılması – gündelik hayatın her yere nüfuz eden ve her tarafa yayılan bir parçası haline geliyor.

Son 3 yıl boyunca, hükümetler ve siyasi partiler tarafından global ölçekte örgütlenen sosyal medya manipülasyonlarını gözlemledik. 2019 raporumuz bilgisayımsal propaganda trendleri ile gelişen araçları, kapasiteleri, stratejileri ve kaynakları analiz etmektedir.

1. 2017'de 28, 2018'de 48, bu yıl ise 70 ülkede meydana gelen organize sosyal medya manipülasyon kampanyalarına dair kanıtlar bulduk. Her ülkede, kamusal tutumları yerel olarak şekillendirmek için sosyal medyayı kullanan en az bir siyasi parti veya devlet kurumu bulunmaktadır. (Model-1)

2. Sosyal medya birçok otoriter rejim tarafından yandaşlaştırıldı. Bilgisayımsal propaganda, 26 ülkede, üç farklı şekilde bilgi kontrol aracı olarak kullanılıyor: Temel insan haklarını ortadan kaldırmak, siyasi muhalifleri itibarsızlaştırmak ve muhalif görüşleri bastırmak. (Model-2)

3. Küçük bir grup komplike devlet aktörü, dış etki operasyonları için bilgisayımsal propaganda kullanıyor. Facebook ve Twitter, dış etki operasyonlarını bu platformları küresel izleyicileri etkilemek için kullanmış olan yedi ülke ile (Çin, Hindistan, İran, Pakistan, Rusya, Suudi Arabistan ve Venezuela) ilişkilendiriyor. (Model-3)

4. Çin, küresel dezenformasyon düzeninde önemli bir oyuncu haline geldi. Hong Kong'daki 2019 protestolarına kadar, Çin'in bilgisayımsal propaganda bulgularının çoğu Weibo, WeChat ve QQ gibi yerel platformlarda gerçekleşti. Ancak Çin'in Facebook, Twitter ve YouTube'un agresif kullanıma yönelik yeni ilgisi demokrasi açısından kaygı uyandırmaktadır.

5. Her zamankinden daha fazla sosyal ağ platformları olmasına rağmen, Facebook hala sosyal medya manipülasyonu için tercih edilen platform olmaya devam ediyor. 56 ülkede, Facebook'ta resmi olarak düzenlenmiş bilgisayımsal propaganda kampanyalarının izine rastladık. (Model-4)

İçindekiler

İllüstrasyon

Bu rapordan alıntı yapılabilir: Samantha Bradshaw ve Philip N. Howard. (2019) Küresel Dezenformasyon Bozukluğu: 2019 Organize Sosyal Medya Manipülasyonunun Küresel Dökümü. Çalışma Raporu 2019.2. Oxford, İngiltere: Bilgisayımsal Propaganda Projesi.

Giriş

Dünya çapında hükümet yetkilileri sosyal medyayı konsensüs yaratmak, yapay zeka temelli baskı oluşturmak ve liberal uluslararası düzene duyulan güveni sarsmak için kullanıyorlar.

Propaganda her zaman politik söylemin bir parçası olmasına rağmen, bu kampanyaların derin ve geniş kapsamı kamu yararına yönelik eleştirel endişeleri artırıyor.

Siber birlikler, kamuoyunu çevrimiçi olarak manipüle etmekle görevlendirilmiş devlet veya siyasi parti aktörleri olarak tanımlanmaktadır (Bradshaw ve Howard 2017a). Dünyadaki siber birliklerin resmi organizasyonunu karşılaştırmalı olarak inceliyoruz ve bu aktörlerin bilgisayımsal propagandayı politik amaçlar için nasıl kullandıklarına bakıyoruz. Bu, bilgisayımsal propagandanın gelişen stratejileri, araçları ve tekniklerine dair bir envanterin çıkarılmasını kapsar. Nefret söylemini veya diğer manipüle edilmiş içerik türlerini güçlendirmek için 'siyasi botların' kullanılmasını, verilerin yasa dışı işlenmesini ya da mikro hedeflemeyi, siyasi muhaliflere-gazetecilere çevrimiçi zorbalık etmek veya onları taciz etmek için bir 'troller ordusu' kurmayı içerir. Ayrıca, dünya genelinde siber birlik kabiliyetlerinin portresini çizmek için kullanılan teknikleri geliştirmede harcanan kapasite ve kaynakları takip ediyoruz.

Sosyal medya aracılığıyla halkın tutumlarını şekillendirmek için kullanılan bilgisayımsal propaganda, birkaç kötü aktörün faaliyetlerinden öte bir anaakım haline geldi.

Yüksek miktarda enformasyon içeren ve buna karşılık kullanıcıların dikkat ve güven düzeyinin sınırlı olduğu bir bilgi ortamında; bilgisayımsal propagandanın araç ve teknikleri, dijital kampanyanın ve kamu diplomasisinin yaygın -ve muhtemelen gerekli- bir parçası haline geliyor.

Küresel ölçekte karşılaştırmalı bir siber birlik etkinliğinin portresini oluşturmaya ek olarak, çevrimiçi siyasetin değişen doğasını nasıl tanımladığımız ve anladığımız; çevrimiçi demokrasiyi ve insan haklarını geliştirmek için teknolojilerin nasıl kullanılabileceği veya kullanılması gerektiği konusunda toplumsal ve bilimsel bir tartışmayı yürütmeyi umuyoruz.

Bu yılki raporda, 70 ülkenin siber birlik faaliyetlerini inceliyoruz: Angola, Arjantin, Ermenistan, Avustralya, Avusturya, Azerbaycan, Bahreyn, Bosna Hersek, Brezilya, Kamboçya, Çin, Kolombiya, Hırvatistan, Küba, Çek Cumhuriyeti, Ekvador, Mısır, Eritre, Etiyopya, Gürcistan, Almanya, Yunanistan, Honduras, Guatemala, Macaristan, Hindistan, Endonezya, İran, İsrail, İtalya, Kazakistan, Kenya, Kırgızistan, Makedonya, Malezya, Malta, Meksika, Moldova, Myanmar, Hollanda, Nijerya, Kuzey Kore, Pakistan, Filipinler, Polonya, Katar, Rusya, Ruanda, Suudi Arabistan, Sırbistan, Güney Afrika, Güney Kore, İspanya, Sri Lanka,

İsveç, Suriye, Tayvan, Tacikistan, Tayland, Tunus, Türkiye, Ukrayna, Birleşik Arap Emirlikleri, Birleşik Krallık, Birleşik Devletler, Özbekistan, Venezuela, Vietnam ve Zimbabve.

Dünya Çapında Artan Bilgisayımsal Propaganda Bulguları

2017'de 28, 2018'de 48, bu yıl ise 70 ülkede organize sosyal medya manipülasyon kampanyalarına dair kanıtlar bulduk. Bu büyümenin bir kısmı; seçimler sırasında bilgisayımsal propaganda araçlarını ve tekniklerini deneyen veya yeni bir bilgi kontrol aracı olarak gören yeni katılımcılardan geliyor. Bununla birlikte gazeteciler, akademisyenler ve aktivistler; resmi olarak örgütlenmiş sosyal medya manipülasyon örneklerini tanımlamak, rapor etmek ve ortaya çıkarmak için dijital araçlarla ve daha keskin bir kelime dağarcığı ile donanmışlardır.

Geçtiğimiz üç yıl boyunca, bilgisayımsal propaganda örneklerini tanımlayabilmek için dilimizi ve arama terimlerimizi geliştirebildik. Son on yılda birçok ülkenin sosyal medya manipülasyonlarını resmi olarak organize ettiğine dair unsurlar bulduk. Sonuç olarak, bilgisayımsal propagandanın dijital bilgi ekosisteminin her yere nüfuz eden ve her tarafa yayılan bir parçası haline geldiğini öne sürüyoruz.

Otoriter Rejimlerde Sosyal Medyanın Kullanımı

Birçok otoriter rejimde bilgisayımsal propaganda; gözetim, sansür ve şiddet tehdidi ile birlikte stratejik bir bilgi kontrol aracı haline geldi. Otoriter ülkelerin gazetecilere, siyasi muhaliflere ve toplumun geniş kesimlerine karşı kullandığı kampanya türlerini kategorize ettik. Bilgisayımsal propagandanın kullanıldığı üç farklı yolu şöyle sıraladık:

(1) Temel insan haklarını ortadan kaldırmak;

(2) Siyasi muhalefeti itibarsızlaştırmak;

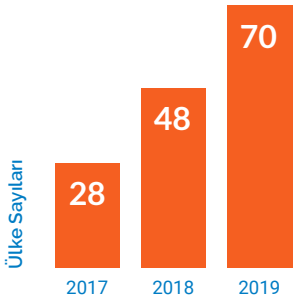
(3) Siyasi muhalefeti bastırmak.

Sosyal medya teknolojilerinin kullanılması otoriter rejimlere; aynı anda dijital kamusal alanları denetler, sansürler ve kısıtlarken kamusal tartışmaları şekillendirmek ve çevrimiçi propagandayı yaymak için güçlü bir araç sağlar.

Komplike Aktörler Tarafından Düzenlenen Sınırlı Sayıdaki Dış Etki Operasyonları

Dış etki operasyonları önemli bir konudur ancak bilgisayımsal propagandayı yabancı devlet aktörlerine atfetmek bir sorun olmaya devam ediyor.

Kendi platformları üzerinden yapılan etki operasyonları hakkında sınırlı bilgi yayınlamaya başlayan Facebook ve Twitter, yedi ülkede - Çin, Hindistan, İran, Pakistan, Rusya, Suudi Arabistan ve Venezuela- dış etki operasyonu ile ilişkilenmiş siber birliklere karşı harekete geçti.



150%

Son iki yılda organize sosyal medya manipülasyon kampanyalarını kullanan ülkelerdeki artış

Bu önlem her ne kadar dış etki operasyonlarının kapsamını karşılamasa da bu oldukça gizli olgunun genel hatlarını çizmeye başladığımızı rahatlıkla söyleyebiliriz.

Çin Yanlış Bilgilendirmedeki Gücünü Gösteriyor

Yakın zamana kadar Çin'in diğer ülkelerde kamuoyunu manipüle etmek için nadiren sosyal medyayı kullandığını gördük. Çin'de bilgisayımsal propaganda esasen Weibo, WeChat ve QQ gibi yerel platformların kullanıcılarına odaklanmıştı.

Ancak 2019'da Çin hükümeti, Hong Kong'un demokrasi savunucularını aşırı radikaller olarak göstermek için küresel sosyal medya platformlarını kullanmaya başladı (Lee Myers ve Mozur 2019). Yurt içindeki platformların ötesinde, küresel sosyal ağ teknolojilerinin artan gelişmişliği ve kullanımı, Çin'in bu teknolojilere jeopolitik güç ve etki aracı olarak nasıl yöneldiğini göstermektedir.

Facebook Hala 1 Numara

Her zamankinden daha fazla sosyal ağ platformu olmasına rağmen, Facebook hala siber birlik etkinlikleri için başlıca platform olmaya devam ediyor.

Bunun nedeni dünyanın en büyük sosyal ağ platformlarından biri olarak pazar büyüklüğünün yanı sıra yakın aile ve arkadaş iletişimi, politik haber ve bilgi kaynağı , grup ve sayfa oluşturma becerisi gibi platformun sağladığı belirli kolaylıklarla açıklanabilir. 2018'den beri Instagram ve YouTube gibi görüntü ve video paylaşım platformlarında daha fazla siber birlik etkinliği kanıtı topladık.

Ayrıca WhatsApp'ta kampanya yürüten siber birliklerin bulgularına da rastladık. Daha fazla insan bu sosyal ağ teknolojilerini politik iletişim için kullandıkça, bu platformların önümüzdeki birkaç yıl içinde daha da önemli hale geleceğini düşünüyoruz.

Şekil 1 - Küresel Dezenformasyon Düzeni

SOSYAL MEDYA MANİPÜLASYONUNA KATILAN ÜLKELER

- Angola
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Bahrain
- Bosnia & Herzegovina
- Brazil
- Cambodia
- China
- Colombia
- Croatia
- Cuba
- Czech Republic
- Ecuador
- Egypt
- Eritrea
- Ethiopia
- Georgia
- Germany
- Greece
- Guatemala
- Honduras
- Hungary
- India
- Indonesia
- Iran
- Israel
- Italy
- Kazakhstan
- Kenya
- Kyrgyzstan
- Macedonia
- Malaysia
- Malta
- Mexico
- Moldova
- Myanmar
- Netherlands
- Nigeria
- North Korea
- Pakistan
- Philippines
- Poland
- Qatar
- Russia
- Rwanda
- Saudi Arabia
- Serbia
- South Africa
- South Korea
- Spain
- Sri Lanka
- Sudan
- Sweden
- Syria
- Taiwan
- Tajikistan
- Thailand
- Tunisia
- Turkey
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uzbekistan
- Venezuela
- Vietnam
- Zimbabwe

İstanbul Üniversitesi
Dijital İletişim
Kulübü
2019 ORGANİZE SOSYAL MEDYA MANİPÜLASYONUNUN KÜRESEL DÖKÜMÜ

ŞEKİL 2 – BİLGİ KONTROL ARACI OLARAK BİLGİSAYIMSAL PROPAGANDA

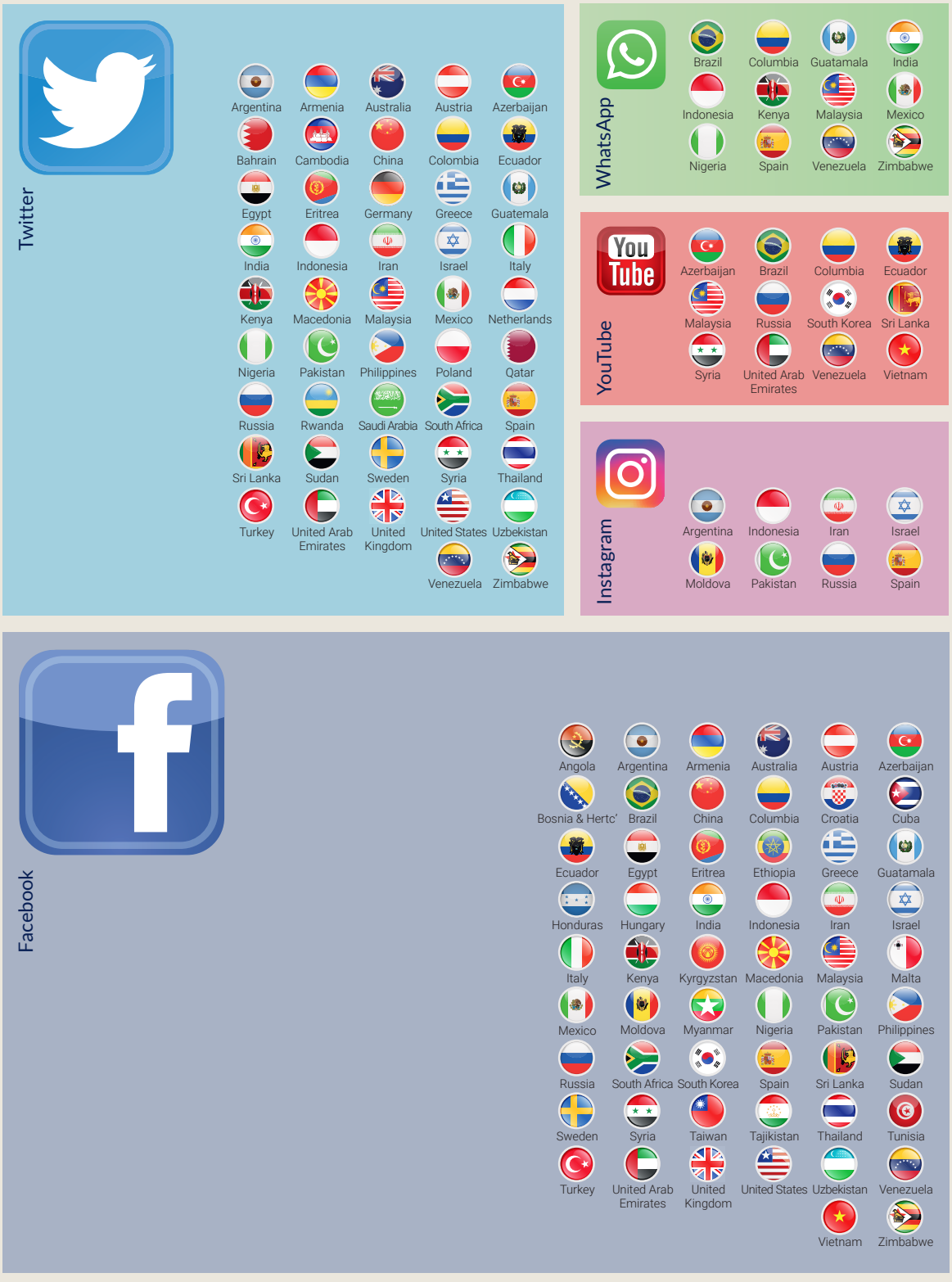
OTORİTER ÜLKELERDE BİLGİSAYIMSAL PROPAGANDANIN YAYILMASI

ŞEKIL 3 – SOSYAL MEDYA ÜZERINDEKİ DIŞ ETKİ OPERASYONLARI

FACEBOOK VE TWITTER YOLUYLA YABANCI ETKİ OPERASYONLARINDA BULUNAN ÜLKELER

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. Not: Facebook ayrıca, açıkça bir hükümete veya siyasi partiye bağlı olmayan 'eşgüdümlü orijinal olmayan davranış' ile ilgili hesapları da reddetmiştir. Bu yayından kaldırmalar Mısır, Makedonya, Kosova, Tayland ve Birleşik Arap Emirlikleri menşeli hesapları içermektedir. Buna ek olarak, Facebook ve Twitter tarafından tanımlanan bazı siber birlik faaliyetleri, Bangladeş ve Honduras gibi, yerel olarak odaklanmıştır ve bu nedenle bu operasyona yabancı operasyonlar dahil edilmemiştir.

ŞEKİL 4 – SOSYAL MEDYA MANİPÜLASYONLARINDA ÖNE ÇIKAN PLATFORMLAR
SİBER BİRLİK AKTİVİTELERİ İÇİN KULLANILAN SOSYAL MEDYA PLATFORMLARI



Raporun Metodolojisi

Bu raporun metodolojisi dört aşamadan oluşmaktadır:

1. Siber birlik faaliyetlerini aktaran haber makalelerinin sistematik içerik analizi;
2. Kamu arşivleri ve bilimsel raporların ikincil literatür taraması;
3. Ülkeler bazında vaka çalışmaları hazırlamak;
4. Uzman görüşleri

Geçtiğimiz üç yıl boyunca, üç aşamalı metodolojimiz, global olarak organize edilen manipülasyon kampanyalarına ışık tutan geniş bir yelpazedeki kamusal belgeleri başarılı bir şekilde tespit etmemizi sağladı.

Kamuoyuna açılmamış siber birlik operasyonları mevcut olmakla birlikte bu vakalar zamanla artış gösterdi.

Bu rapordaki amacımız, devlet aktörlerinin bu alanda nasıl faaliyet gösterdiğinin tam bir görünümünü ortaya koymak olmasa da halka açık bilgileri bir araya getirerek daha büyük bir resim oluşturmaya başlayabiliriz.

Ülkeye özgü profillerinin, haber öğelerinin ve ikincil literatür kaynaklarının tam listesi 2019 rapor ana sayfasında bulunabilir.

İçerik analizi, iletişim ve medya çalışmalarında yerleşik bir araştırma yöntemidir (Herring 2009). İnternet ve sosyal medyanın; siyasal eylem, rejim dönüşümü ve dijital kontrol ile nasıl etkileşime girdiğini anlamak için kullanılır. (Bradshaw ve Howard 2018a, 2017b; Edwards, Howard ve Joyce 2013; Joyce, Antonio ve Howard 2013; Strange ve diğ. 2013). Bu nitel içerik analizi, kamuoyunu manipüle etmek için aktif olarak sosyal medyayı kullanan devlet aktörlerinin çeşitliliğini, bunların kapasitelerini, stratejilerini ve kaynaklarını anlamak için kullanıldı. İçerik analizimizi geçen yılın raporundan sonra, haber makalelerindeki belirli değişkenlerin kodlanmış elektronik tablosunu oluşturmak için amaçlı örneklemi kullanarak modelledik.

Aşağıdaki anahtar kelimeler seçildi ve çalışmamızla uyumlu olarak kullanıldı: bot; Cambridge Analytica; dezenformasyon; Facebook; sahte hesap; enformasyon savaşı; Instagram; askeri; yanlış bilgilendirme; propaganda; psikolojik operasyonlar; sosyal medya; çorap kukla; trol; Twitter; WhatsApp; Youtube.

Nitel içerik analizlerimizi yürütmede iki önemli kısıtlama mevcut: medya yanlılığı ve dil. Yanlılığı hafifletmek için, LexisNexis'i ve çeşitli profesyonel, yerel ve amatör haber kaynaklarına tıklanma sağlayan ilk üç arama motoru sağlayıcısını (Google, Yahoo, Bing) kullandık. Veri kümemizin yalnızca yüksek kaliteli haber kaynakları kullanılarak oluşturulduğundan emin olmak için, her makaleye bir güvenilirlik puanı verdik.

Bir numarada sıralanan makaleler, büyük, profesyonel markalı haber kuruluşlarından geldi. İki numarada sıralanan makaleler daha küçük profesyonel haber kuruluşlarından, yerel haber kuruluşlarından veya uzman yorumlarından ve profesyonel bloglardan geldi. Üç numarada sıralanan makaleler içerik çiftliklerinden veya kişisel ya da radikal partizan bloglardan geldi. Bu makaleler örneklemden çıkarıldı.

Dil, nitel içerik analizimizi yürütmede ikinci bir sınırlama idi. Bu yılki küresel envanter için; Arapça, İngilizce, Fransızca, Almanca, Yunanca, Macarca, İtalyanca, Farsça, Lehçe, Portekizce, Rusça ve İspanyolca dilinde yazılmış haber makaleleri ve ikincil kaynaklar üzerinde durduk. Ayrıca Bosna, Hırvatistan, Gürcistan, Kazakistan, Kırgızistan, Malezya, Kuzey Makedonya, Tayvan, Tacikistan, Türkmenistan, Özbekistan'a ait haber makalelerinin çeviri hizmetlerinin yanı sıra siber birlik faaliyetleri ile ilgili yüksek kaliteli haber ve bilgilerin toplanması ve kümelenmesi için ek bir portal sunan BBC monitoring ile çalıştık.

Şu ülkeler için yalnızca İngilizcede rapor edilenlere dayandık: Ermenistan, Azerbaycan, Kamboçya, Çin, Çek Cumhuriyeti, Eritre, Etiyopya, Macaristan, İsrail, Moldova, Myanmar, Hollanda, Kuzey Kore, Pakistan, Filipinler, Sırbistan, Güney Kore, Sri Lanka, Tayland, Türkiye ve Vietnam.

İçerik analizi yapıldıktan sonra, bir araştırma görevlisi ekip; belirli bir ülke bağlamında siber birlik faaliyetinin derinlemesine profilini oluşturmak için **ikincil bir literatür taraması** yaptı.

Bu vaka çalışmaları; içerik analizinden toplanan verilerden ve vaka çalışması yazarlarının siber birlik etkinliği hakkındaki diğer yüksek kaliteli, açık kaynaklı bilgileri aradığı derinlemesine ikincil literatür taramasından alınmıştır.

Bu çalışma; hükümet raporları, think tank raporları, akademik ve bilimsel çalışmaları ve sivil toplum örgütleri tarafından yürütülen araştırmalara bakmayı içeriyordu.

Bu raporda kullanılan haber kaynaklarının ve ikincil literatürün tüm arşivi, çevrimiçi Zotero veri tabanında bulunabilir. Umarız bu genel erişime açık kütüphane gelecekteki araştırmalara ilham verebilir.

Nitel içerik analizi ve ikincil literatür taramasının tamamlanmasından sonra; araştırma görevlileri, bulguları **ülke bazlı kısa vaka çalışmalarıyla** sentezlemiştir. Vaka çalışmaları, içerik analizinde tanımladığımız bilgisayımsal propaganda örneklerinin yanı sıra sosyal medya manipülasyonlarının gerçekleştiği belirli ülke bağlamları ve medya ortamları hakkında daha fazla bilgi sağlar. İçerik analizine ve ikincil literatür incelemesine ek olarak, raporun yanı sıra çevrimiçi ek bir veri olarak bulunabilecek ülkelerin yüzde 84'ü için bir vaka çalışması gerçekleştirdik.

Son olarak, araştırma metodolojimizin son adımı olan -**uzman görüşleri**- vaka çalışmalarının bilirkişi değerlendirmesinden geçmesine imkan verdi. Ayrıca İngilizce, yerel dildeki haberciliğin ve bulduğumuz ikincil literatürünün niteliğine dair geri bildirim almamızı; alternatif dillerdeki ek kaynakları ve alıntıları ana dilindeki konuşmacılarla tartışmamızı sağladı.

Uzmanlardan; araştırma görevlileri tarafından hazırlanan örnek olay incelemelerini gözden geçirmeleri ve:

(1) bilgilerin ve verilerin doğruluğunu kontrol etmeleri;

(2) açık kaynak materyalleri için ek alıntılar sağlamaları;

(3) verinin güvenilirliği hakkında genel geri bildirimde bulunmaları istendi.

Polonya, Sri Lanka, Tayvan, Tunus ve Ukrayna vakalarında, içerik analizi ve literatür incelemesinden toplanan veriler konusunda uzmanlara başvurduk.

1 https://monitoring.bbc.co.uk/

Organizasyon Şekli

Siber topluluk aktiviteleri birçok organizasyon şekline sahiptir. Çeşitli aktörler sosyal medyayı; kamuoyunu şekillendirmek, siyasal gündem belirlemek ve fikirleri yaymak üzere kullanmaktadır.

Sosyal medya üzerindeki bilgisayımsal propaganda birçok ülkede artış gösterirken, bu artışın belirli bir aktöre atfedilmesi zordur.

Bu raporda, sosyal medyayı kamuoyunu manipüle etmek için kullanan; siber birliklere -hükümetlere veya siyasî partilere- odaklanacağız.

44 ülkede hükümet organlarının kamu davranışını şekillendirmek için bilgisayımsal propaganda kullandıklarına dair kanıtlar bulduk.

Bu kategori iletişim ve dijital bakanlıkları veya askeri kampanyaları içermekte. Freedom House'a göre "özgür olmayan" olarak kabul edilen ülkelerde, bir bakanlığın veya iktidar partisinin, davranışları yerel ölçekte şekillendirmek üzere bilgisayımsal propaganda kullandığına dair kanıt bulduk.

Birkaç demokrasideyse hükümet veya askeri inisiyatiflerin izine rastladık. Bu rapor için Birleşik Krallık'ta Facebook grupları kuran ve "itibarsızlaştırma, güvensizlik yayma, caydırma, yıldırma, geciktirme ve aksatma" (Greenwald 2015) için tasarlanmış, ikna etmeye yönelik iletişim içerikli Youtube videoları üreten Ortak Tehdit Araştırmaları İstihbarat Grubu (JTRIG)'nun aktivitelerini hesaba kattık.

Ayrıca Birleşik Devletler'de bulunan, Küba'da sahte sosyal ağ yaratan (Greenwald 2014) Amerika Birleşik Devletleri Uluslararası Kalkınma Ajansı (USAID) programı gibi aktiviteleri de hesaba kattık. Daha fazla diyaloğu mümkün kılmasını umuyoruz.

Bilgisayımsal propaganda siyaset, milli güvenlik ve istihbarat operasyonları için giderek yaygınlaşan bir araç haline gelmektedir. Bu örneklerin devlet aktörlerinin bu araçları uygun, demokratik ve kabul edilebilir bir şekilde kullanmaları yönünde

Hükümetlere ve askeri teşebbüslere ek olarak, siyasi partileri de inceledik. 70 ülkenin 45'inde seçimler esnasında bilgisayımsal propaganda araç ve tekniklerini kullanan seçimlerde adaylığını koymuş siyasi partilere veya siyasetçilere rastladık. Burada; Amerika Birleşik Devletleri'nde Mitt Romney (Carroll 2012), Avustralya'da Tony Abbott (Rolfe 2013) ve Hollanda'da Geert Wilders (Blood 2017) gibi sahte takipçi toplayan siyasetçi örneklerini de hesaba kattık.

Ayrıca, Hindistan'da olduğu gibi (Gleicher 2019), manipüle edilmiş medya içeriği ile hedef seçmen kitlesine reklam yapan parti örneklerini ve Birleşik Krallık Brexit referandumunda Cambridge Analytica (Cadwalladr 2017) firmasının ayrılma oyu yönünde yaptığı gibi illegal mikro-hedeflemelerin örneklerini dikkate aldık. Son olarak, Brezilya'da (Rio 2018), Hindistan'da (Dwoskin and Gowen 2018) ve Nijerya'daki (Hitchen et al. 2019) Whatsapp kampanyaları gibi siyasi partilerin bilinçli olarak sosyal ağlarda dezenformasyonu yayma veya büyütmeye yönelik faaliyetlerini de hesaba kattık.

Manipülasyon kampanyalarının organizasyonundaki önemli bir özellik de siber birliklerin genellikle özel sektör, sivil toplum kuruluşları, internet alt kültürleri, gençlik grupları, hacker kolektifleri, aşırı gruplar, sosyal medya influencer'ları ve ideolojik olarak kendilerini destekleyen gönüllülerle işbirliği halinde çalışmalarıdır.

Bu gruplar arasında bir ayrım yapılması; özellikle faaliyetlerin dolaylı veya dolaysız olarak devlet tarafından onaylanması durumunda oldukça zorlaşıyor.

Bu raporda, uyuşan ideolojiler veya hedefler sebebiyle dolaylı olarak onaylanmış olma ihtimali bulunan kampanyalardan ziyade devlet tarafından resmen onaylanan resmî koordinasyon veya faaliyetlerin izini süreceğiz.

70 ülkeden 25'inde, özel şirketlerle veya bilgisayımsal propaganda hizmeti sunan stratejik iletişim firmalarıyla çalışmış devlet aktörlerine rastladık. 70 ülkenin 30'unda hükümet ve sivil toplum teşkilatları arasında resmî koordinasyona rastladık. Azerbaycan, İsrail, Rusya, Tacikistan ve Özbekistan'daki gibi bazı vakalarda, öğrenci veya gençlik grupları bilgisayımsal propaganda yaptırılmak üzere hükümet organlarınca istihdam edilmektedir.

TABLO 1 - ORGANİZASYON ŞEKLİ VE SOSYAL MEDYA MANIPÜLASYONUNUN YAYGINLIĞI

Ülkeler	Hükümet Ajansları	Politikacılar ve Partiler	Girişimciler Girişim	Sivil Toplum Kuruluşları	Vatandaşlar ve Fenomenler
Angola	■	■			
Argentina	■	■■	■		
Armenia	■				
Australia		■■			
Austria		■■	■		
Azerbaijan	■			■	■
Bahrain	■■		■■		■
Bosnia & Herzegovina	■				
Brazil		■■	■■		■
Cambodia	■■	■			■
China	■■		■	■	
Colombia		■	■■		
Croatia		■			
Cuba	■			■	
Czech Republic		■			
Ecuador		■■			
Egypt	■	■			■
Eritrea	■				
Ethiopia	■				
Georgia	■		■	■	
Germany		■		■	
Greece		■			
Guatemala	■	■	■■		■
Honduras	■				
Hungary	■				
India		■■	■■	■	■
Indonesia		■	■		
Iran	■■				■
Israel	■■	■		■■	
Italy		■■			■
Kazakhstan	■	■			
Kenya		■■	■■		
Kyrgyzstan		■	■		■
Macedonia		■			■
Malaysia	■■	■■	■■	■	■

Ülkeler	Hükümet Ajansları	Politikacılar ve Partiler	Özel Girişimciler	Sivil Toplum Kuruluşları	Vatandaşlar ve Fenomenler
Malta	■	■	■		
Mexico		■■	■■	■	
Moldova	■	■			
Myanmar	■				
Netherlands		■			
Nigeria	■	■	■		
North Korea	■■				
Pakistan	■	■■			
Philippines	■	■■	■■	■	■
Poland		■	■		
Qatar	■				
Russia	■■		■	■	
Rwanda	■	■			
Saudi Arabia	■		■■	■	■
Serbia	■	■		■	
South Africa		■	■■		
South Korea		■■			
Spain		■		■	
Sri Lanka	■	■■			
Sudan	■			■	
Sweden		■			
Syria	■■		■	■	
Taiwan		■■	■		
Tajikistan	■				■
Thailand	■				■
Tunisia		■			
Turkey	■	■			■
Ukraine	■			■	
United Arab Emirates	■■		■■	■■	■
United Kingdom	■	■	■		
United States	■■	■	■■		
Uzbekistan	■			■	■
Venezuela	■■	■	■■	■	
Vietnam	■				■
Zimbabwe		■			

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. Not: Bu tablo, sosyal medyayı etkileyen siyasi aktörlerin türlerini ve bu kuruluşların örneklerinin sayısını bildirmektedir. Devlet kurumları, siyasi partiler, sivil toplum grupları ve özel yükleniciler için, ■ = bir kuruluş bulundu, ■■ = iki kuruluş bulundu, ■■ = üç veya daha fazla kuruluş bulundu. Bu araçları kullanan bireysel vatandaş sayısını değerlendirmek zor olduğundan, vatandaş kullanımına ilişkin kanıtlar ■ ile belirtilmektedir.

Stratejiler, Araçlar ve Teknikler

Propaganda hakkında pek yeni bir şey olmamasına karşın, sosyal ağ teknolojilerinin sağladığı olanaklar –algoritmalar, otomasyon ve büyük veri- dijital çağda bilgi iletiminin ölçek, kapsam ve kesinliğini değiştirmektedir.

87%
kişisel hesaplar kullanan ülkeler

80%
bot hesaplar kullanan ülkeler

11%
sayborg hesaplar kullanan ülkeler

7%
hacklenmiş veya çalınmış hesaplar kullanan ülkeler

Hesap Tipleri

Sahte hesaplar, siber birliklerce bilgisayımsal propaganda yaymak üzere kullanılmaktadır. Son üç yılda, üç sahte hesap tipinin yaygınlığını gözlemledik: bot hesap, kişisel hesap ve sayborg hesap. Botlar, çevrimiçi insan davranışını taklit etmesi için tasarlanmış otomatik hesaplardır. Genellikle anlatıyı güçlendirmek veya muhaliflerin sesini bastırmak üzere kullanılırlar. Bu tip bot hesapların 70 ülkenin 50'sinde kullanıldığına rastladık. Bununla birlikte, botlardan daha yaygın olarak, otomasyon kullanmayan kişilerin yönettiği hesaplara rastladık. Bu hesaplar otomasyon yerine yorum veya tweet yazarak sohbet ya da sosyal medya platformları üzerinden özel mesajlaşma ile meşgul olurlar. Bu yılın raporunda 70 ülkenin 60'ında kişilerin yönettiği hesaplar tespit ettik. Otomasyonu insan seçimiyle harmanlayan sayborg hesaplar ise tanımladığımız bir diğer hesap çeşididir.

Bu yıl, hacklenmiş ya da çalınmış hesapları da sahte hesaplar tipolojimize ekledik. Aslında bu hesaplar kendi başlarına sahte olmasalar da, yüksek profilli hesaplar siber birlikler tarafından hak sahibinin hesaba erişimini engelleyerek hükümet yanlısı propaganda yaymak ya da ifade özgürlüğünü sansürlemek amacıyla stratejik olarak kullanılıyor. Az sayıda devlet aktörü, çalınmış veya hacklenmiş hesapları kampanyalarının bir parçası olarak kullanmaya başladı. Bu da bilgisayımsal propagandanın daha geleneksel siber saldırı biçimleriyle olan bağlantısallığına işaret ediyor.

Son olarak, siber birlik aktivitelerinde kullanılan tüm hesapların sahte olmadığını belirtmek gerekir. Vietnam veya Tacikistan gibi bazı ülkelerdeki devlet aktörleri hükümet yanlısı propagandayı yaymak, siyasî muhalifleri trollemek veya toplu şikayet için siber birlikleri kendi gerçek hesaplarını kullanmaya teşvik etmektedir. Sosyal medya şirketleri siber birlik aktiviteleriyle bağlantılı hesapları kapatmada agresifleştikçe gerçek hesapların kullanılması daha da öne çıkan bir strateji haline gelebilir.

TABLO 2 – SAHTE HESAP TÜRLERİ

Ülkeler	Botlar	İnsan	Sayborg	Hacklenmiş
Angola	●			
Argentina	●	●		
Armenia	●	●		
Australia	●	●		
Austria	●	●		
Azerbaijan	●	●		
Bahrain	●	●		
Bosnia & Herzegovina		●		
Brazil	●	●	●	
Cambodia	●			
China	●	●		
Colombia	●	●		
Croatia		●		
Cuba	●			
Czech Republic		●		
Ecuador		●		
Egypt	●	●		
Eritrea		●		
Ethiopia		●		
Georgia	●	●		
Germany	●	●	●	
Greece	●	●		
Guatemala	●	●		●
Honduras		●		
Hungary	●	●		
India	●	●		
Indonesia	●	●		
Iran	●	●		●
Israel	●	●		
Italy	●			
Kazakhstan	●	●		
Kenya	●	●		
Kyrgyzstan		●		
Macedonia	●	●		
Malaysia	●			

Ülkeler	Botlar	İnsan	Sayborg	Hacklenmiş
Malta	●	●		
Mexico	●	●	●	
Moldova	●	●		
Myanmar	●	●		
Netherlands	●			
Nigeria	●	●		
North Korea		●		●
Pakistan	●	●		
Philippines	●	●		
Poland	●			
Qatar	●			
Russia	●	●	●	●
Rwanda		●		
Saudi Arabia	●	●	●	
Serbia	●	●		
South Africa	●	●		
South Korea	●	●		
Spain	●	●		
Sri Lanka	●	●	●	
Sudan		●		
Sweden	●	●		
Syria	●	●		
Taiwan	●			
Tajikistan		●		
Thailand	●	●		
Tunisia	●	●		
Turkey	●	●		
Ukraine	●	●		
United Arab Emirates	●	●		
United Kingdom	●	●	●	
United States	●	●	●	
Uzbekistan		●		●
Venezuela	●	●		
Vietnam		●		
Zimbabwe	●	●		

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. Not: Bu tablo, 2010-2019 yılları arasında belirlenen sahte hesap türlerini bildirmektedir. Sahte sosyal medya hesap türleri için: otomatikleştirilmiş hesaplar, =kişisel hesaplar, = sayborg hesaplar, = çalınmış hesaplar, = kanıt bulunamadı.

71%

hükümet veya parti yanlısı propaganda yaymak

89%

siyasi muhaliflere saldırmak için bilgisayımsal propaganda kullanmak

34%

toplumdaki bölünmeleri yönlendirmek için tasarlanmış kutuplaştırıcı mesajlar yaymak

Mesajlaşma ve Duygu Değeri

Siber birlikler diğer kullanıcılarla çevrimiçi iletişim kurarken çeşitli mesajlaşma ve duygu değeri stratejileri kullanmaktadır. Duygu değeri; bir mesajın, olayın veya bir şeyin ne kadar çekici veya itici olduğunu ifade eder. 2019 raporu için, siber birliklerin çevrimiçi kullanıcılarla sohbet ederlerken kullandıkları mesajlaşma ve duygu değeri stratejileri tipolojimizi şu şekilde genişlettik:

(1) Hükümet veya parti yanlısı propaganda yaymak;
(2) Muhalefete saldırmak veya lekeleme kampanyaları düzenlemek;
(3) Dikkat dağıtmak veya sohbeti ya da eleştiriyi önemli konulardan saptırmak;
(4) Ayrışma ve kutuplaşma yaratmak;
(5) Kişisel saldırı veya taciz yoluyla katılımı bastırmak.

Tablo 3 – Mesajlaşma ve Birleşme Değeri

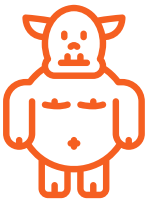
Ülkeler	Destek	Muhalefete Saldırı	Dikkat Dağıtıcı	Fikir Ayrılığı	Baskı Altına Almak
Angola		✓			
Argentina	✓	✓		✓	✓
Armenia		✓	✓	✓	✓
Australia	✓	✓			
Austria		✓			✓
Azerbaijan	✓	✓			✓
Bahrain	✓	✓		✓	✓
Bosnia & Herzegovina	✓	✓	✓	✓	✓
Brazil	✓	✓	✓	✓	✓
Cambodia	✓	✓			
China	✓	✓	✓		✓
Colombia	✓	✓		✓	
Croatia				✓	
Cuba	✓	✓			✓
Czech Republic		✓			
Ecuador		✓	✓		✓
Egypt	✓	✓			✓
Eritrea		✓			✓
Ethiopia	✓	✓			
Georgia	✓	✓			✓
Germany	✓	✓		✓	
Greece		✓			✓
Guatemala	✓	✓			✓
Honduras	✓				
Hungary	✓	✓	✓	✓	✓
India	✓	✓		✓	
Indonesia	✓	✓		✓	
Iran	✓	✓			✓
Israel	✓				
Italy			✓	✓	
Kazakhstan	✓	✓	✓		
Kenya	✓	✓			
Kyrgyzstan	✓	✓			✓
Macedonia		✓		✓	✓
Malaysia	✓	✓			✓

Ülkeler	Destek	Muhalefete Saldırı	Dikkat Dağıtıcı	Fikir Ayrılığı	Baskı Altına Almak
Malta		✓			✓
Mexico	✓	✓			✓
Moldova	✓	✓		✓	
Myanmar	✓	✓		✓	✓
Netherlands				✓	
Nigeria		✓			✓
North Korea	✓	✓			
Pakistan	✓	✓			✓
Philippines	✓	✓		✓	✓
Poland		✓			
Qatar	✓				
Russia	✓	✓	✓	✓	✓
Rwanda		✓			✓
Saudi Arabia	✓	✓		✓	✓
Serbia	✓	✓			✓
South Africa	✓	✓			✓
South Korea	✓	✓			
Spain		✓		✓	
Sri Lanka	✓	✓		✓	✓
Sudan		✓			✓
Sweden				✓	
Syria	✓	✓	✓		✓
Taiwan	✓	✓	✓		
Tajikistan	✓	✓			✓
Thailand	✓	✓			✓
Tunisia	✓	✓			
Turkey	✓	✓			✓
Ukraine	✓	✓			✓
United Arab Emirates	✓	✓			✓
United Kingdom	✓	✓	✓	✓	
United States	✓	✓	✓	✓	✓
Uzbekistan		✓			✓
Venezuela	✓	✓	✓		✓
Vietnam	✓	✓			✓
Zimbabwe	✓	✓			✓

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. Not: Bu tablo 2010-2019 yılları arasındaki siber birlik aktivitelerinin; mesajlaşma ve birleşme değerlerinin stratejileri hakkında rapor vermektedir.
Sosyal medya raporları için: ✓ = destekleyici, ✓ = muhalefete saldırı, ✓ =dikkat dağıtıcı ✓ = fikir ayrılığı, ✓ = baskı altına almak, ✓ = kanıt bulunamadı.

75%

kullanıcıları yanlış yönlendirmek için dezenformasyon ve medya manipülasyonu kullanıldı



68%

devlet destekli troller; siyasi muhalifleri, muhalefeti ve gazetecileri hedef almak için kullanıldı

73%

hashtagler işgal edilerek mesaj ve içerik kuvvetlendirildi

İletişim Stratejileri Siber birlikler bir dizi iletişim stratejileri kullanmaktadır. Bu aktiviteleri 4 kategoride sınıflandırdık

(1) Dezenformasyon veya manipüle edilmiş medyanın yaratılması
(2) Hesapların veya içeriğin topluca şikayet edilmesi
(3) Veri odaklı stratejiler
(4) Trolleme, doxing (sanal ortamda kişisel bilgilere ulaşma) veya taciz
(5) İçeriği ve çevrimiçi medyayı güçlendirme

Dezenformasyon veya manipüle edilmiş medyanın yaratılması, en yaygın iletişim stratejisidir. İncelediğimiz 70 ülkenin 52'sinde siber birlikler; kullanıcıları yanlış yönlendirmek için caps'ler, videolar, sahte haber siteleri veya manipüle edilmiş medya gibi içerikleri aktif olarak üretmiştir.

Bazen siber birliklerce yaratılan içerik, belirli toplulukları veya kullanıcı kesimlerini hedef almaktadır. Kullanıcılar hakkında çevrimiçi veya çevrimdışı veri kaynaklarını kullanarak ve popüler sosyal medya platformlarında reklam bedelini ödeyerek, bazı siber birlikler dezenformasyon ve manipüle edilmiş medya ile belirli toplulukları hedef alır.

Trolleme, doxing (sanal ortamda kişisel bilgilere ulaşma) veya taciz giderek büyüyen küresel bir sorun ve temel insan haklarına yönelik tehdittir. 2018'de, sosyal medya aracılığıyla siyasî muhalefete veya aktivistlere saldırma amacıyla devlet destekli trolleri kullanan 27 ülke tespit etmiştik. Bu yıl, 47 ülke trolleri kendi dijital cephanelerinin bir parçası olarak kullandı. Siber birlikler ayrıca bir içeriğin, hesabın konuşmasını veya ifadesini toplu-şikayet yoluyla sansürlemekte. Aktivistlerin, siyasî muhalefetin veya gazetecilerin gönderileri genellikle koordine bir siber birlik ağıyla şikayet ediliyor ki sosyal medya şirketlerinin uygunsuz içeriği kaldırmak üzere kullandığı otomatik sistemler devreye girebilsin.

Trolleme, hesapların kapatılması veya gönderilerin silinmesi gerçek dünya şiddeti ile birlikte gerçekleşebilir. Bu durum temel insan haklarının ifadesi üzerinde derin ve ürpertici bir etkiye sahip olabilmektedir.

Tablo 4 – İletişim Stratejileri

Ülkeler	Dezenformasyon	Kitleleri Raporlama	Veri Tabanlı Stratejiler	Trolller	İçerik Kuvvetlendirme
Angola	●			●	●
Argentina	●		●	●	●
Armenia	●	●		●	●
Australia					●
Austria	●		●	●	●
Azerbaijan	●	●		●	●
Bahrain				●	●
Bosnia & Herzegovina	●			●	●
Brazil	●		●	●	●
Cambodia	●				●
China	●	●		●	●
Colombia	●			●	
Croatia	●				●
Cuba	●			●	●
Czech Republic					
Ecuador	●	●		●	
Egypt	●			●	●
Eritrea				●	
Ethiopia	●			●	
Georgia	●			●	●
Germany	●			●	●
Greece	●			●	●
Guatemala	●	●		●	●
Honduras	●		●		●
Hungary	●			●	●
India	●		●	●	●
Indonesia	●				●
Iran	●	●	●	●	●
Israel	●		●		
Italy	●				●
Kazakhstan	●				●
Kenya	●		●		●
Kyrgyzstan				●	
Macedonia	●				●
Malaysia	●		●		●
Malta	●			●	
Mexico	●	●	●	●	●
Moldova	●		●	●	●
Myanmar	●			●	●
Netherlands	●				●
Nigeria	●		●	●	
North Korea	●				
Pakistan	●		●		●
Philippines	●			●	●
Poland				●	
Qatar					●
Russia	●	●	●	●	●
Rwanda				●	
Saudi Arabia	●			●	●
Serbia	●			●	●
South Africa	●		●	●	●
South Korea					●
Spain	●				
Sri Lanka	●			●	●
Sudan		●		●	
Sweden	●			●	●
Syria	●			●	●
Taiwan			●	●	
Tajikistan				●	●
Thailand				●	
Tunisia	●				●
Turkey		●		●	●
Ukraine	●			●	●
United Arab Emirates	●		●	●	●
United Kingdom	●		●		●
United States	●		●		●
Uzbekistan				●	
Venezuela	●			●	●
Vietnam	●	●		●	●
Zimbabwe	●			●	

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. **Not:** Bu tablo siber birlikler tarafından kullanılan iletişim stratejilerini raporlamaktadır. İletişim stratejileri için: =dezenformasyon ve manipüle edilmiş medya, = içeriğin / hesapların toplu raporlanması, = veriye dayalı stratejiler, = trollemek, = içeriğin güçlendirilmesi, = kanıt bulunamadı.

Organizasyonel Bütçe, Davranışlar ve Kapasite

Siber birliklerin boyutu ve operasyonları hakkında halka açık kısıtlı bilgi bulunmasına karşın; bütçelerinin ne kadar olduğu, nasıl iş birliğinde bulundukları ve organizasyonel kapasite türleri ile benimsedikleri davranışların resmini çizmek üzere parçaları birleştirmeye başladık.

Takım Büyüklüğü ve Sürekliliği

Takımların büyüklüğü ve sürekliliği ülkeden ülkeye değişkenlik göstermektedir. Bazı ülkelerde takımlar, seçimler veya başka önemli siyasî etkinlikler süresince kamu davranışını şekillendirmek üzere geçici olarak görünmektedir. Diğer ülkelerdeyse, siber birlikler tam zamanlı çalışarak çevrimiçi sohbetleri ve bilgiyi kontrol etmek, sansürlemek ve şekillendirmek üzere medya ve iletişim mecralarına entegre olmuş halde. Bazı takımlar yüzlerce sahte hesabı yöneten bir avuç insandan oluşuyor. Çin, Vietnam veya Venezuela gibi diğer ülkelerdeyse kalabalık takımlar çevrimiçi kanallar yoluyla aktif bir şekilde kamuoyunu şekillendirmek ve söylemi denetlemek için devletlerce istihdam ediliyor.

Bütçe ve Harcamalar

Bilgisayımsal propaganda büyük sermayelerle sürdürülüyor. 'PR' veya stratejik iletişim firmalarına, Filipinler (Mahtani ve Cabato 2019), Guatemala (Currier ve Mackey 2018) ve Suriye (York 2011) gibi ülkelerde kampanyalar yapmaları için yüklü meblağlarda para harcandığını saptadık. Bu kontratlar milli butik veya bölgesel firmalara yapılan daha küçük harcamalardan Cambridge Analytica (örneğin Kazeem 2018) gibi küresel şirketlerle yapılan multi-milyon dolarlık sözleşmelere kadar geniş bir aralığa sahip olabilir. Troll endüstrisindeki yükseliş kamusal ve akademik ilginin genişleyen bir alanıdır. Aynı zamanda gelecek çalışmalar ve basın araştırmalarına açık bir alandır.

Bilgi ve Beceri Dağıtımı

Formel ve enformel bilginin dağılmasının coğrafi sınırları aşarak gerçekleştiği görüldü. Örneğin Myanmar'da siber birlik aktivitesi incelemeleri esnasında askeri yetkililerin Rus teknisyenlerce sosyal medya kullanımı üzerine eğitildiğinin bulgularına rastladık (Mozur 2018). Benzer bir şekilde, Sri Lanka'daki siber birlikler Hindistan'da resmî eğitim aldı (Expert consultation 2019). Ayrıca sızdırılmış e-postalar, Etiyopya'daki Information Network Agency'nin (Enformasyon Ağı Ajansı) personelini resmî eğitim almak üzere Çin'e gönderdiğini gösterdi (Nunu 2018). Bilgisayımsal propagandaya dair bilgi ve becerilerinin küresel ölçekte nasıl yayıldığına dair birçok boşluk bulunsa da, bu konu gelecekte inceleme ve basın araştırmalarını bekleyen önemli bir alandır.

Siber Birlik Kapasitesi

Siber birliğin kullandığı davranışlara, harcamalara, araçlara ve kaynaklara karşılaştırılmalı olarak bakarak, küresel sosyal medya manipülasyonu organizasyonunun daha karşılaştırmalı bir resmini oluşturmaya başlayabiliriz. Ulusal bağlamların daima dikkate alınması gerekir. Bununla birlikte, bu olguya ilişkin geniş ve karşılaştırmalı bir anlayış geliştirmek için rejim türleri boyunca cereyan eden organize dezenformasyon kampanyalarına dair deneyimlerin genelleştirilmeye değer olduğunu düşünüyoruz. Siber birlik ekiplerinin birbirleriyle ilişkilerini karşılaştırmalı olarak değerlendirmek için; faaliyete karışan devlet aktörlerinin sayısını, araçların karmaşıklığını, kampanya sayısını, ekiplerin büyüklüğünü ve kalıcılığını, yapılan bütçe ve harcamaları dikkate alarak basit bir ölçü geliştirmeye başladık. Siber birlik aktivitelerini 4 ölçekte tanımlıyoruz.

1- Minimal Düzeydeki Siber Birlik Takımları yeni kurulmuş ya da önceden aktif olan ancak mevcut faaliyetleri belirsiz olan ekiplerdir. Yeni oluşturulmuş ekipler minimal düzeyde kaynaklara sahiptir ve bilgisayımsal propagandanın yalnızca birkaç aracını kısıtlı sayıdaki platformda uygulayabilir. Küçük çaptaki siber birlik aktiviteleri aynı zamanda, bilgisayımsal propaganda araçlarını deneyimlemiş sadece bir veya iki politikacı gördüğümüz ülkeleri içerir. Bu ekipler yurt dışı operasyonlarda bulunmadan yerel bağlamda faaliyet gösterirler. Küçük ekipler şu ülkeleri kapsar; Angola, Arjantin, Ermenistan, Avustralya, Hırvatistan, Ekvador, Yunanistan, Hollanda, Güney Kore, İsveç, Tayvan ve Tunus.

2- Düşük Düzeyli Siber Birlik Kapasitesi, seçimler veya referandum sırasında aktif olabilen ancak bir sonraki seçim dönemine kadar faaliyetini durduran küçük ekipleri içerir. Düşük düzeyli ekipler, dezenformasyonu artırmak için botların kullanılması gibi yalnızca birkaç strateji deneme eğilimindedirler. Bu ekipler yurt dışı operasyonlarda bulunmadan yerel bağlamda faaliyet gösterirler. Düşük kapasiteli ekipler; Avusturya, Kolombiya, Çek Cumhuriyeti, Eritre, Almanya, Honduras, Macaristan, Endonezya, İtalya, Kenya, Makedonya, Moldova, Nijerya, Kuzey Kore, Polonya, Ruanda, Sırbistan, Güney Afrika, İspanya, Zimbabve gibi ülkeleri kapsar.

3- Orta Düzeyli Siber Birlik Kapasitesi, bilgi alanını kontrol etmek için yıl boyu istihdam edilen çok daha tutarlı bir forma ve stratejiye sahip ekipleri içerir. Bu ekipler genellikle birçok aktör türü ile eş güdümlü çalışır ve sosyal medya manipülasyonu için çok çeşitli araçları ve stratejileri dener. Bazı orta kapasiteli ekipler yurt dışı etki operasyonları yürütür. Orta düzeyli ekipler; Azerbaycan, Bahreyn, Bosna Hersek, Brezilya, Kamboçya, Küba, Etiyopya, Gürcistan, Guatemala, Hindistan, Kazakistan, Kırgızistan, Malezya, Malta, Meksika, Pakistan, Filipinler, Katar, Sri Lanka, Sudan, Tacikistan, Tayland, Türkiye, Ukrayna, Birleşik Krallık ve Özbekistan gibi ülkeleri kapsar.

4- Yüksek Düzeyli Siber Birlik Kapasitesi, psikolojik operasyonlar ve bilgi savaşlarında istihdam edilen çok sayıda çalışanı ve yüksek bütçeli harcamaları içerir. Kullanılan çok sayıda tekniğin yanı sıra, AR-GE'ye yönelik önemli fon harcamaları da olabilir. Bu takımlar sadece seçim sürecinde operasyon yürütmez, aynı zamanda bilgi alanını şekillendirmeye tahsis edilmiş tam zamanlı çalışanları içerir. Bu birlikler hem yurt içi hem de yurt dışı operasyonlara odaklanır. Yüksek kapasiteli ekipler; Çin, Mısır, İran, İsrail, Myanmar, Rusya, Suudi Arabistan, Suriye, BAE, Venezuela, Vietnam ve ABD'yi içerir.

TABLO 5 – SİBER BİRLİK KAPASİTELERİ

YÜKSEK KAPASİTE

Ülke	Durum	Takım Büyüklükleri, Eğitim ve Harcamalara Dair Notlar
Çin	Kalıcı	Yerel ve bölgesel ofislerde çalışan kişilerin oluşturduğu ekiplerin tahmini büyüklüğü: 300.000-2.000.000 kişi
Mısır	Kalıcı	–
İran	Kalıcı	FB reklamlarına 6 bin dolar harcandı
İsrail	Kalıcı	400 kişilik ekip büyüklüğü tahminleri. Örgün eğitim bulguları. 778 bin ve 100 milyon dolar değerinde birden fazla sözleşme.
Myanmar	Kalıcı	Rusya'da örgün eğitim bulguları.
Rusya	Kalıcı	–
Suudi Arabistan	Kalıcı	Twitter hashtag trendleri için 150 Pound tahmini maliyet
Suriye	Kalıcı	4 bin dolar değerinde birden fazla sözleşme
BAE	Kalıcı	10 milyon doların üzerinde çeşitli harcamalar
ABD	Kalıcı & Geçici	–
Venezuela	Kalıcı	500 kişilik çoklu ekiplerin takım büyüklüğü tahminleri
Vietnam	Kalıcı & Geçici	10 bin kişinin takım büyüklüğü tahminleri

TABLO 5 – SİBER BİRLİK KAPASİTELERİ

ORTA KAPASİTE

Ülke	Durum	Takım Büyüklükleri, Eğitim ve Harcamalara Dair Notlar
Azerbaycan	Kalıcı	–
Bahreyn	Kalıcı	32 milyon dolar değerinde birçok sözleşme
Bosna Hersek	Geçici	–
Brezilya	Geçici	10 milyon, 130 bin, 24 bin, 12 milyon Brezilya Reali değerinde birçok sözleşme.
Kamboçya	Kalıcı & Geçici	–
Küba	Kalıcı	–
Etiyopya	Kalıcı	Çin'de eğitim bulguları. Tahmini aylık maaşlar / 300 dolar
Gürcistan	Geçici	–
Guatemala	Kalıcı	100 bin dolar değerinde birçok sözleşme
Hindistan	Geçici	50-300 kişiden oluşan birden fazla ekip. 1.4 milyon doların üzerinde çoklu sözleşme ve reklam harcamaları
Kazakistan	Kalıcı	–
Kırgızistan	Kalıcı & Geçici	50 kişilik ekip büyüklüğü tahmini. 2 bin dolar değerinde birçok sözleşme. Günlük maaşların 3-4 dolar olduğu tahmin edilmekte.
Malezya	Kalıcı	50-2000 kişi arasında personel olduğu tahmin ediliyor. Örgün eğitim kanıtları bulundu.
Malta	Kalıcı	–
Meksika	Geçici	–
Pakistan	Kalıcı	–
Filipinler	Kalıcı	300-500
Katar	Geçici	–
Sri Lanka	Kalıcı & Geçici	Hindistan'da örgün eğitim bulguları
Sudan	Kalıcı	–
Tacikistan	Kalıcı	400 kişilik takım büyüklüğü tahmini
Tayland	Kalıcı	Örgün eğitim bulguları
Türkiye	Kalıcı	500 kişilik takım büyüklüğü tahmini
Ukrayna	Kalıcı	20 bin kişilik takım büyüklüğü tahmini
Birleşik Krallık	Geçici	Ayrılma kampanyaları için Cambridge Analytica'ya 3.5 milyon sterlin harcandı
Özbekistan	Kalıcı	–

TABLO 5 – SİBER BİRLİK KAPASİTELERİ

DÜŞÜK KAPASİTE

Ülke	Durum	Takım Büyüklükleri, Eğitim ve Harcamalara Dair Notlar
Avusturya	Geçici	–
Kolombiya	Geçici	–
Çek C.	Geçici	–
Eritre	Kalıcı	–
Almanya	Geçici	–
Honduras	Geçici	–
Macaristan	Geçici	–
Endonezya	Geçici	1-50 milyon Rupi değerinde birçok sözleşme
İtalya	Geçici	–
Kenya	Geçici	Cambridge Analytica ile yapılan 6 milyon ABD Doları değerinde bir sözleşme
Makedonya	Geçici	–
Moldova	Geçici	Facebook ve Instagram reklamlarına 20 bin dolar değerinde harcama
Nijerya	Geçici	Cambridge Analytica ile yapılan 2.8 milyon ABD Doları değerinde bir sözleşme
Kuzey Kore	Kalıcı	200 kişilik takım büyüklüğü tahmini
Polonya	Geçici	–
Ruanda	Geçici	–
Sırbistan	Kalıcı	Aylık maaş tahminleri 370 euro
Güney Afrika	Geçici	2 milyon dolar değerinde birçok sözleşme
İspanya	Geçici	–
Zimbabve	Geçici	–

MİNİMAL KAPASİTE

Ülke	Durum	Takım Büyüklükleri, Eğitim ve Harcamalara dair Notlar
Angola	Geçici	–
Arjantin	Geçici	30-40 personel. 2015'te 14 ve 11 milyon pezo değerinde birçok sözleşme. 2017'de 200 milyon pezo.
Ermenistan	Geçici	–
Avustralya	Geçici	–
Hırvatistan	Geçici	–
Ekvador	Etkinlik Yok	200 bin dolar değerinde birçok sözleşme
Yunanistan	Geçici	–
Hollanda	Geçici	–
Güney Kore	Etkinlik Yok	Daha önceden aktif olan 80 kişiden az takım
İsveç	Geçici	–
Tayvan	Etkinlik Yok	–
Tunus	Geçici	–

Kaynak: Yazarların toplanan verilere dayalı değerlendirmeleri. Not: Bu tablolar siber birlik aktörlerinin kapasitesini raporlamaktadır.

SONUÇ

Bir zamanlar özgürlük ve demokrasi için bir güç olarak ilan edilen sosyal medya; dezenformasyonu artıran, şiddete sevk eden, medya ve demokratik kurumlara olan güveni azaltan bir rol oynaması bakımından, artan bir denetim altına girmiştir.

Bu rapor, devlet kurumlarının ve siyasi partilerin sosyal medyayı; siyasi propaganda yaymak, dijital bilgi ekosistemini kirletmek, ifade ve basın özgürlüğünü baskılamak için ne şekillerde kullandığını gösterdi. Sosyal medyanın olanakları dezenformasyon ölçeğini, kapsamını ve kesinliği artırmaya yardımcı olsa da (Bradshaw ve Howard 2018b), bilgisayımsal propagandanın kalbindeki birçok meselenin- kutuplaşma, güvensizlik ya da demokrasinin düşüşü- sosyal medyadan ve hatta internetin kendisinden bile önce var olduğunun bilinmesi önemlidir. Sosyal medya teknolojilerinin yandaşlaştırılması- ama aynı zamanda demokratik toplumların yaşadığı köklü sorunlar da- dünyadaki demokrasiler için endişe yaratmalıdır. Bilgisayımsal propaganda dijital kamuoyunun olağan bir parçası haline geldi. Yapay Zeka, Sanal Gerçeklik ve Nesnelerin İnterneti gibi toplumu ve siyaseti kökten değiştirmeye hazır yeni teknolojilerle bu teknikler gelişmeye devam edecek.

Fakat bilgisayımsal propaganda demokrasiye karşı köklü sorunların bir belirtisi olduğundan çözümlerin bu sistemik zorlukları göz önünde bulundurması önemlidir. Sosyal medya platformalarının güncel bilgi ortamını şekillendirmede oynadığı rolün de dikkate alınması gereklidir. Öte yandan, sosyal medya platformlarının mevcut enformasyon ortamını şekillendirmedeki rolünün düşünülmesi gerekir. Güçlü bir demokrasi yüksek kalitede bilgiye erişmeyi, vatandaşların bir araya gelip bir konuyu görüşmesini ve tartışmasını, bir konu üzerinde düşünmesini, karşılıklı duyguların paylaşılmasını ve buna izin verilmesini gerektirir. Sosyal medya platformları gerçekten halkın müzakere edebilmesi ve demokrasi için bir alan yaratıyor mu? Yoksa vatandaşları bağımlı, yanlış bilgilendirilmiş ve agresif hale getiren içeriği mi güçlendiriyor?

Referanslar

Blood, David. 2017. **Is Social Media Empowering Dutch Populism?** *The Financial Times*. https://www.ft.com/content/b1830ac2-07f4-11e7-97d1-5e720a26771b.

Bradshaw, Samantha, and Philip N. Howard. 2017a. **The Global Organization of Social Media Disinformation Campaigns**. Journal of International Affairs 71(1.5).

Bradshaw, Samantha, and Philip N. Howard. 2017b. **Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation**. Oxford: Oxford Internet Institute. Working Paper.

———. 2018a. **Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation**. COMRPOP Working Paper Series 2018(1): 26.

Bradshaw, Samantha, and Philip N. Howard. 2018b. **Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life**. Knight Foundation Working Paper. https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

Cadwalladr, Carole. 2017. **The Great British Brexit Robbery: How Our Democracy Was Hijacked**. *The Guardian*. http://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Carroll, Rory. 2012. **Fake Twitter Accounts May Be Driving up Mitt Romney's Follower Number**. *The Guardian*. https://www.theguardian.com/world/2012/aug/09/fake-twitter-accounts-mitt-romney.

Currier, Cora, and Danielle Mackey. 2018. **The Rise of the Net Center: How an Army of Trolls Protects Guatemala's Corrupt Elite**. *The Intercept*. https://theintercept.com/2018/04/07/guatemala-anti-corruption-trolls-smear-campaign/ (August 5, 2019).

Dwoskin, Elizabeth, and Annie Gowen. 2018. **On WhatsApp, Fake News Is Fast — and Can Be Fatal**. *Washington Post*. https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html (September 3, 2019).

Edwards, Frank, Philip N. Howard, and Mary Joyce. 2013. **Digital Activism & Non-Violent Con lict**. http://digital-activism.org/2013/11/report-on-digital-activism-and-non-violent-conflict/ (May 17, 2017).

Gleicher, Nathaniel. 2019. **Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan**. https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/.

Greenwald, Glenn. 2014. **The 'Cuban Twitter' Scam Is a Drop in the Internet Propaganda Bucket**. *The Intercept*. https://theintercept.com/2014/04/04/cuban-twitter-scam-social-media-tool-disseminating-government-propaganda/ (April 10, 2017).

———. 2015. **Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research**. *The Intercept*. https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/ (April 10, 2017).

Herring, Susan C. 2009. **Web Content Analysis: Expanding the Paradigm**. In *International Handbook of Internet Research*, eds. Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen. Springer Netherlands, 233–49. http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_14 (May 17, 2017).

Hitchen, Jamie, Jonathan Fisher, Nic Cheeseman, and Idayat Hassan. 2019. **How WhatsApp Influenced Nigeria's Recent Election — and What It Taught Us about 'Fake News**. *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/ (September 3, 2019).

Joyce, Mary, Rosas Antonio, and Philip N. Howard. 2013. **Global Digital Activism Data Set**. http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34625/version/2.

Kazeem, Yomi. 2018. **Cambridge Analytica Tried to Sway Nigeria's Last Elections with Buhari's Hacked Emails**. Quartz. https://qz.com/1234916/cambridge-analytica-tried-to-sway-nigerias-last-elections-with-buharis-hacked-emails/.

Lee Myers, Steven, and Paul Mozur. 2019. **China Is Waging a Disinformation War Against Hong Kong Protesters**. New York Times. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html (September 3, 2019).

Mahtani, Shibani, and Regine Cabato. 2019. **Why Crafty Internet Trolls in the Philippines May Be Coming to a Website near You**. *Washington Post*. https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html (September 4, 2019).

Mozur, Paul. 2018. **A Genocide Incited on Facebook, With Posts From Myanmar's Military**. The New York Times. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (July 24, 2019).

Nunu. 2018. **Leaked Documents Show That Ethiopia's Ruling Elites Are Hiring Social Media Trolls (And Watching Porn) · Global Voices**. *Global Voices*. https://globalvoices.org/2018/01/20/leaked-documents-show-that-ethiopias-ruling-elites-are-hiring-social-media-trolls-and-watching-porn/ (July 24, 2019).

Rio, I. T. S. 2018. **Computational Power: Automated Use of WhatsApp in the Elections**. ITS FEED. https://feed.itsrio.org/computational-power-automated-use-of-whatsapp-in-the-elections-59f62b857033 (March 2, 2019).

Rolfe, John. 2013. **Fake Twitter Followers for Tony Abbott Being Investigated by Liberal Party**. Perth Now. https://www.perthnow.com.au/politics/federal-politics/fake-twitter-followers-for-tony-abbott-being-investigated-by-liberal-party-ng-90b331e9e3ca2542ec9cbdf6d994f986.

Strange, Austin et al. 2013. **China's Development Finance to Africa: A Media-Based Approach to Data Collection**. Working Paper. https://www.cgdev.org/publication/chinas-development-finance-africa-media-based-approach-data-collection (May 17, 2017).

York, **Jillian C**. 2011. **Syria's Twitter Spambots**. *The Guardian*. https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution (April 10, 2017).

TEŞEKKÜR

Yazarlar, Avrupa Araştırma Konseyi'nin "Bilgisayımsal Propaganda: Algoritmaların ve Botların Avrupa'da Siyasal Söylem Üzerindeki Etkisinin Araştırılması," (Öneri 648311, 2015–2020, Baş Araştırmacı Philip N. Howard) araştırma projesine vermiş olduğu destek için teşekkürlerini sunar. Bu çalışmaya ayrıca destekleri için Hewlette, Luminate ve Adessium Vakıflarına teşekkür ederiz. Bu çalışmada ifade edilen tüm görüş, bulgu, sonuç veya tavsiyeler yazarlara aittir ve fon sahipleri, Oxford İnternet Enstitüsü veya Oxford Üniversitesi'nin görüşlerini yansıtmak zorunda değildir.

Ön verileri toplayan ve bu raporda bahsi geçen ülkeler için sosyal medya manipülasyonu hakkında ülke profillerini çıkaran Ualan Campbell-Smith, Amelie Henle, Caio Machado ve Cailean Osborne'a araştırmadaki yardımları ve tavsiyeleri için müteşekkiriz. Ayrıca Akın Ünver, Alberto Lalama, Alexi Abrahams, Angelina Huyun, Arzu Geybulla, Ben Nimmo, Bence Kollanyi, Chris Roper, Darko Brkan, Didac Fabregas-Badosa, Gabby Lim, Ingrid Grodnig, Iva Nenedic, Lisa-Maria Neudert, Marc Owen Jones, Martin Becerra, Mimie Liotsiou, Monika Kaminska, Nahema Marchal, Nick Monaco, Niki Cheong, Olivier Milland, Philip Di Salvo, Ralph Schroeder, Biberiye Ajayi, Sabine Niederer, Sanjana Hattotuwa, Vidya Narayanan, Tamar Kintsurashvili ve Tom Sear'e ve bunun yanı sıra bu proje için başvurduğumuz çok sayıda uzmana minnettarız. Rapor için destek aldığımız kişilerin ülkelere özgü uzmanlıkları; verilerimizin güvenilirliği ve geçerliliğini sağlamak için çok önemliydi. Ülke profillerini inceleme hususundaki yardımları ve ayırdıkları zaman için; ayrıca bu rapora dahil edilen ek kaynaklar, alıntılar ve veri noktalarının temini için onlara teşekkür ediyorum.

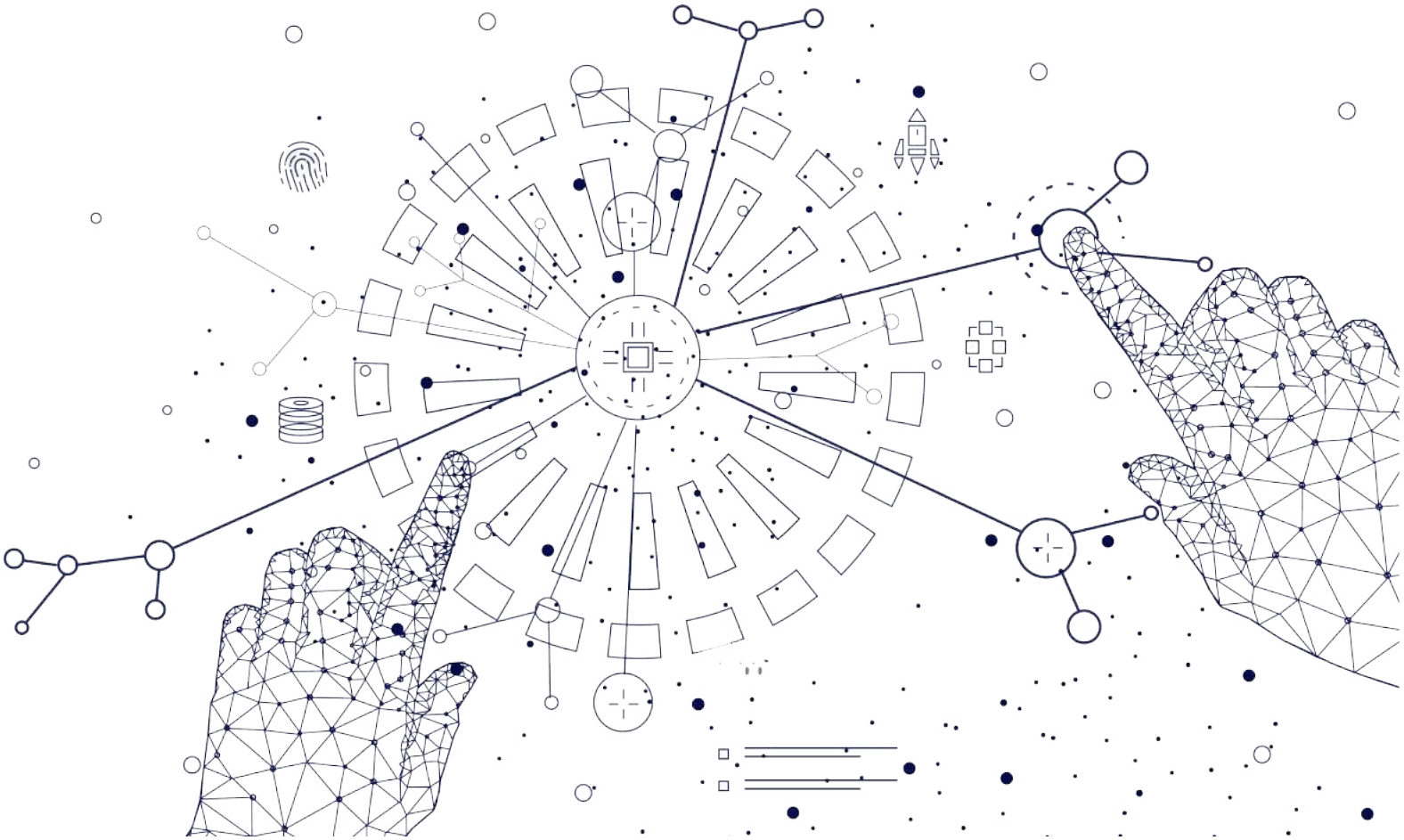
YAZAR BİYOGRAFİLERİ

SAMANTHA BRADSHAW teknoloji ve demokrasi konusunda önde gelen bir uzmandır. Bradshaw'ın tez araştırması; dezenformasyon üreticileri ve kullanıcılarını, ve teknolojinin - yapay zeka, otomasyon, büyük veri analizi- çevrimiçi dezenformasyonun yayılmasını nasıl arttırdığını ve kısıtladığını inceler. Sosyal medya ve demokrasi arasındaki karmaşık ilişkiyi inceleyen, analiz eden ve açıklayan teorik ve metodolojik yaklaşımların önde gelen çalışmalarından Samantha'nın araştırması, teknolojinin politik ifade ve mahremiyet üzerindeki etkisiyle ilgili akademik tartışma, kamusal anlayış ve politika tartışmalarının ilerletilmesine yardımcı olmuştur.

Samantha, doktorasını Oxford Üniversitesi, Oxford İnternet Enstitüsü'nde tamamlıyor. Kendisi aynı zamanda Bilgisayımsal Propaganda Projesi Araştırmacısı. Samantha "@sbradshaww" tweeter hesabını kullanmaktadır.

PHILIP N. HOWARD profesör ve yazardır. Oxford Üniversitesi'nde ders vermekte ve Oxford İnternet Enstitüsü'nü yönetmektedir. Balliol Koleji'nde profesördür. Bilgi politikaları ve uluslararası ilişkiler hakkında yazılar yazmaktadır. "The Managed Citizen", "Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up", ve en son çıkan "Computational Propaganda" adlı sekiz kitabın yazarıdır. Birden fazla "en iyi kitap" ödülü kazanmıştır. Araştırma ve eleştiri yazıları New York Times, Washington Post ve birçok uluslararası medya kuruluşunda yer almıştır. Foreign Policy dergisi 2018'de onu 'Küresel Düşünür' olarak adlandırdı ve National Democratic Institute, sahte haberlerin sosyal bilimine öncülük ettiği için kendisine "Demokrasi Ödülü" verdi. Bir sonraki kitabı "Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives" 2020 yılının başlarında Yale Üniversitesi Yayınları'ndan çıkıyor.

www.philhoward.org adresinde blog yazmakta ve "@pnhoward" tweeter hesabını kullanmaktadır.



İstanbul Üniversitesi
Dijital İletişim
Kulübü

Editör:
Ömer Faruk Özbil

Çevirenler:
Çağla Ayaz
Çağdaş Sarıpınar
Ümit Kuş

Redaktör:
Yeşim Akmeraner Kökat

Tasarım:
Mehmet Taha Ersöz

Bilgisayımsal Propaganda Projesi

Oxford İnternet Enstitüsü

Oxford Üniversitesi

1 St Giles • Oxford OX1 3JS

Website: www.oii.ox.ac.uk