

İTERNET YÖNETİŞİMİNE GİRİŞ

7. Baskı

Jovan Kurbalija

Çeviren
Doç. Dr. İzzet Gökhan Özbilgin

DiPLO

İNTERNET YÖNETİŞİMİNE GİRİŞ

Jovan Kurbalija

Çeviren
Doç.Dr.İzzet Gökhan Özbilgin

diPLO

DiploFoundation (2016) tarafından yayınlanmıştır.

Malta	: DiploFoundation Anutruf, GroundFloor Hriereb Street Msida, MSD 1675, Malta
İsviçre	: DiploFoundation 7bis, Avenue de la Paix CH-1211 Geneva, Switzerland
Sırbistan	: DiploCentar Braničevska 12a/12 11000 Belgrade, Serbia
E-posta	: diplo@diplomacy.edu
Web sitesi	: www.diplomacy.edu
Tasarım ve Düzenleme	: Viktor Mijatović
Gözden Geçiren	: Mary Murphy
Çizimler	: Dr Vladimir Veljasević
Ön Baskı	: Aleksandar Nedeljkov
Basımevi	: Anıl Grup Matbaacılık / www.anilmatbaa.com.tr
Basımevi Sertifika No.	: 40349
Baskı Tarihi	: Kasım 2019

Aksi ifade edilmedikçe bu çalışma aşağıdaki adreste lisanslıdır. <http://creativecommons.org/licenses/by-nc-nd/3.0/>

Bu kitabın diğer dillere tercümesi ve yayınlanması desteklenmektedir.
Daha fazla bilgi için lütfen diplo@diplomacy.edu ile iletişime geçiniz.

Bu kitaptaki belirli bir kısma yapılan atıflar yalnızca bir örnek teşkil etmektedir ve kitabın kendisi tarafından bir onay veya tavsiye olarak düşünülmemelidir.

 Kitabın muhtelif alt bölümlerinde sunulan köşe ikonları ve köprü bağlantıları Cenevre İnternet Platformu (GIP) Dijital Saat gözlemesinde çevrim içi daha fazla (devam eden gelişmeler, araçlar, kaynaklar gibi) materyalin bulunduğuna işaret etmektedir.

Para ile Satılamaz.

ISBN: 978-605-80156-0-9

İçindekiler

SUNUŞ	5
ÖNSÖZ	7
GİRİŞ	9
İnternet Yönetişimi ne anlama gelir?	10
İnternet Yönetişiminin Evrimi	12
İnternet Yönetişimi Bilişsel Araç Kiti	23
Politika yaklaşımları	24
Analojiler	31
İnternet yönetişimi meselelerinin sınıflandırılması	36
ALTYAPI SEPETİ	44
Telekomünikasyon altyapısı	45
İnternet Servis Sağlayıcılar	49
İletişim Kontrol Protokolü / İnternet Protokolü	51
Alan Adı Sistemi	55
Kök bölgesi ve kök sunucular	60
Ağ tarafsızlığı	62
Teknik ve web standartları	71
Bulut bilişim	74
Nesnelerin İnterneti	79
Yakınsama	82
GÜVENLİK SEPETİ	94
Siber güvenlik	94
Siber suç	108
Kritik altyapı	110
Siber terörizm	112
Siber çatışma ve savaş	114
Şifreleme	116
Spam	119
Dijital imzalar	123
Çevrimiçi çocuk güvenliği	125
YASAL SEPET	138
Yasal enstrümanlar	138
Yargı	143
Alternatif uyumsuzluk çözümleri	146
Fikri mülkiyet hakları	148
Telif hakkı	149
Ticari markalar	152

Patentler.....	153
İş hukuku.....	153
Aracılar	155
EKONOMİK SEPET.....	164
E-ticaret	165
İnternet VERİ ekonomisi.....	170
İnternet ERIŞİM ekonomisi.....	171
Ortaya çıkan trendler: Nesnelerin İnterneti, yapay zeka, paylaşımlı ekonomi	173
E-bankacılık, e-para ve sanal para	174
Tüketicinin korunması.....	179
Vergilendirme.....	180
KALKINMA SEPETİ.....	188
Dijital teknolojiler ve kalkınma: politika çerçeve	189
BİT toplumun gelişimini nasıl etkiler?	190
Dijital uçurum	191
Kapasite geliştirme	197
SOSYOKÜLTÜREL SEPET	204
İçerik politikası.....	204
Çevrimiçi eğitim	210
Kültürel çeşitlilik.....	211
Çok dillilik.....	212
Küresel kamu yararı.....	215
İNSAN HAKLARI SEPETİ	222
Çevrim dışı insan haklarına karşı çevrimiçi insan hakları	222
Teknoloji ve insan hakları.....	222
İnternetle sağlanan ‘yeni’ insan hakları	223
İnternet ve mevcut insan hakları.....	225
İfade özgürlüğü ve bilgi alma, alma ve bilgi verme hakkı	225
Mahremiyet ve veri koruması	226
Dijital dünyada çocuk hakları	231
Engelli kişilerin hakları.....	233
Cinsiyet ve çevrimiçi insan hakları.....	223
İNTERNET YÖNETİŞİMİ AKTÖRLERİ	240
Hükümetler	240
İş dünyası.....	250
Sivil toplum	253
Uluslararası organizasyonlar	254
Teknik toplum	255
EKLER.....	261
Diplo hakkında	261
GIP hakkında.....	262
GIP Digital Watch hakkında.....	263
SÖZLÜK.....	264

SUNUŞ

Elinizdeki kitap yaşamımızın hemen her anında olan, sürekli bağılı olduğumuz, ama her nedense üzerinde çok konuşmadığımız, arka tarafında neler olup bittiğini araştırmadığımız bir konuyu ele alıyor: İnternet, İnternet'in paydaşları, İnternet'in yönetilmesi kısaca İnternet Yönetişimi.

İnternet Yönetişimi kamu kurumları, iş dünyası ve sivil toplum kuruluşlarının ilgili rolleri doğrultusunda aktif katılımları ile şekillenen ve kabul edilmiş ilkelerin paylaşımı ile evrenselleşen İnternet kullanımına ilişkin süreçlerdir. Dr. Kurbaliya'nın kitabı, İnternet Yönetişimi hakkında, ekonomik, hukuksal ve teknolojik açıdan uluslararası yapılan çalışmaların geniş okuyucu kitlesine hitap edecek şekilde hazırlanmış olması nedeniyle çok önemlidir. Bu nedenle sadece bilişimcilere değil, hukukçulara, ekonomistlere ve özellikle de akademisyenlere rehberlik edecek bir çalışmadır.

Ülkemizde gerek kamu gerekse özel sektörün İnternet Yönetişimi konusuna bakış açısı henüz tam net değil iken, böyle bir kitabın Türkçe'mize kazandırılması büyük önem arz etmektedir. Çünkü kitap, İnternet Yönetişimi hakkındaki önemli sorulara pratik çözümler sağlamakta, farklı alanlardaki okuyuculara hitap etmekte ve çeşitli şekillerle desteklenerek bir o kadar da yalın bir anlatım sunmaktadır. Kitabın bir diğer öne çıkan özelliği de, her bölüm başında mutlaka ilgili konu hakkında genel bilgilendirme yaptıktan sonra, farklı görüş ve yaklaşımlar hakkındaki tartışmaları açık bir çerçevede sunmasıdır.

İnternet Yönetişimi içeriği bakımından oldukça önemli konuları içeren bir kitaptır. Bu konuları daha detaylı inceleyecek olursak;

- Giriş bölümünde tanımlar yer almakta ve İnternet Yönetişiminin tarihsel gelişimi hakkında bilgi verilmektedir.
- Altyapı sepeti başlıklı ikinci bölümde İnternetin işleyişi ile ilgili daha çok teknik konuların anlatımına yer verilmektedir.
- Güvenlik sepeti başlıklı bölümde, siber güvenlik ve siber suçlara ilişkin bilgi verilmektedir.

- İnternetin hızlı gelişimini belirli bir kalıba sokmanın çok zor olduğu günümüzde Yasal Sepet bölümü, İnternet Yönetişimine ilişkin hâlihazırda uygulanmış veya uygulanabilecek çeşitli yasal düzenlemeler ele almaktadır.
- İnternet üzerinden yapılan ticaret hacmindeki artış sonucunda, e-ticaret kavramı önem kazanmış ve kitabın Ekonomi sepeti bölümünde tüketicinin korunmasından vergilendirmeye, dijital imzalardan e-bankacılığa kadar ekonomi ile ilgili konular geniş kapsamda açıklanmıştır.
- İnternetin bireysel düzeyden küresel düzeye kadar, güç ve kalkınma dağılımına olan etkisi Kalkınma sepeti adı verilen beşinci bölümde incelenmiştir.
- Sosyokültürel sepet başlığı altında, içerik kontrolü, çevrim içi eğitim, kültürel çeşitlilik gibi sosyal ve kültürel alanlarda yaşanan değişimler ele alınmaktadır.
- İnsan Hakları sepetinde, çevrim içi insan hakları, çevrim içi çocuk güvenliği gibi insan hakları ile ilgili konular yer almaktadır.
- Son bölüm olan İnternet Yönetişimi Aktörlerinde ise İnternet Yönetişimi konusunda dünya çapında çalışmalarda bulunan aktörler anlatılmıştır.

Kitap sadece teknolojik içeriğe sahip olmayıp, İnternetin yönetişimi ile ilgili farklı alanlarda küresel bilgiler vermektedir. Üniversitelerde, liselerde ders kitabı olabilecek bir eser olmasının yanı sıra bilgi ve iletişim teknolojileri, hukuk, ekonomi, kamu yönetimi gibi farklı alanlardaki gerek düzenleyiciler gerekse uygulayıcılar için bir başucu kitabı niteliğindedir. Bu nedenledir ki ona yakın dile çevrilerek dünya çapında okunan bir kitap olmuştur. Kitap, dili ve yaklaşımı itibarıyla dijital dönüşüm sürecinde yer alan her kademedeki yöneticiye hitap etmektedir.

Uluslararası kabul görmüş böyle bir kitabı Türkçe'ye çevirmenin mutluluğunu ve gururunu yaşamaktayım. Bu bakımdan en önce Dr. Kurbalija'ya bu değerli eserinin Türkçe'mize kazandırılması konusunda gösterdiği yardımlardan dolayı teşekkür ederim. Bu çalışmanın hazırlanma sürecinde büyük destek veren değerli hocam Prof. Dr. Doğan Nadi Leblebici ve değerli dostum Mustafa Ünver'e, öğrettikleri ile akademik hayatımda ilerlememi sağlayan tüm saygıdeğer hocalarıma, değerli katkıları ile bana yol gösteren bilişim dünyasındaki mesai arkadaşlarıma teşekkürü bir borç bilir, sonsuz şükranlarımı sunarım. Ayrıca bugün sahip olduğum her şeyi borçlu olduğum canım anneme, varlığıyla bana her zaman güç veren değerli abime ve gösterdiği sevgi, sabır ve hoşgöründen dolayı biricik eşime, bana en zor anlarımda yaşama sevinci katan oğullarıma sonsuz teşekkür ederim.

Dijital dönüşüm yolunda bir nebze katkı sağlayabilmek benim için en büyük mutluluk olacaktır.

Okuma ve bilgilendirme sürecinin tadını çıkarmanız dileğiyle...

Doç. Dr. İzzet Gökhan ÖZBİLGİN

Önsöz

2004 yılında, arkadaşlarıma İnternet Yönetişimi Çalışma Grubu (WGIG) üyesi olarak ne yaptığımı anlattığımda beni genellikle yazıcılarını tamir etmek veya yeni yazılımları yüklemek için çağırıyorlardı. Onlara göre, bilgisayarlarla ilgili bir şeyler yapıyordum. WGIG üyelerine ne yaptıklarını arkadaşlarına, eşlerine ve çocuklarına nasıl anlattıklarını soran hızlı bir anket yaptım. Benim gibi onlar da bu konuda zorlanıyorlardı. Bu durum, Diplo'nun İnternet yönetişimi ile ilgili ilk metin ve çizimlerini tasarlamaya ve hazırlamaya başlama sebeplerinden birisidir.

Sekiz yıl sonra bugün ise, yazıcılarını kurmamı isteyen aynı insanlar, artık Facebook üzerinde verilerinin gizliliğini nasıl koruyacakları ya da çocuklarının güvenli olarak İnternet'de nasıl gezebileceklerine ilişkin sorularla bana geliyorlar. Hatta yaşadıkları şehir ve ülkelerde meydana gelebilecek muhtemel bir siber savaş veya baraj, elektrik hatları gibi kritik altyapılara ilişkin çevrimiçi risklerden artan şekilde endişe etmekte. Hepimiz ne kadar yol katetmişiz!

İnternet yönetişimi halkın ilgisini giderek daha da çekmektedir. Modern toplum İnternet'e daha fazla bağımlı hale geldikçe, İnternet yönetişimiyle de o kadar ilişkili olacaktır. İnternet yönetişimi, sadece küçük bir kesimi değil, ister İnternet kullanan 3,6 milyar kişiden biri olalım, istersek de kullanmayan ama sunduğu servislerden faydalanan biri olalım bir şekilde hepimizi ilgilendirecektir.

İnternet yönetişimi elbette ki, e-dünyaya (e-iş, Facebook gibi) derinden entegre olmuş kimseleri daha çok ilgilendirmekle birlikte artık çok daha geniş bir alana hitap etmektedir. Kamu çalışanları, askeri personel, avukatlar, diplomatlar, kamusal mal ve hizmetleri sunan veya kamu düzenini koruyan diğer tüm kesimleri de etkilemektedir. Başta mahremiyet ve insan haklarının korunması olmak üzere, İnternet yönetişimi sivil toplum eylemcileri ve sivil top-

lum örgütleri için de kritik bir konudur. Dünya genelinde akademisyenler ve girişimciler için ise İnternet yönetiřimi, İnternet'in geliřmeye ve yenilięe açık bir ortam olarak kalmasını saęlamalıdır. Yarının Google, Skype, Facebook ve Twitter'ının yaratıcı mucitleri oralarda bir yerlerde İnternet'de gezinmektedirler. Onların İnternet kullanımı için yeni, daha yaratıcı yollar geliřtirme konusunda eřit imkânlara sahip olup olmamaları konusu tarafsız tartiřma aęlarında ve fikri mülkiyet forumlarında sıcak bir řekilde tartiřılmaktadır.

Umarım bu kitap, İnternet yönetiřimi ile ilgili açık ve anlaşılabilir bir giriş saęlar. Bazılarınız bu konu ile ilk defa karřılařacaklar. Dięerleri için ise, kendi uzmanlık alanlarında (e-saęlık, e-ticaret, e-yönetiřim, e-her neyse) zaten yapmış oldukları řeyin İnternet yönetiřimi konularının geniř kapsamının bir parçası olduęuna dair bir hatırlatıcı olabilir.

Böylesi farklı bir yaklařımın altında yatan temel amaç dünyadaki milyarlarca insan için İnterneti entegre ve kolaylařtırıcı araç olarak muhafaza etme konusunda mütevazi bir katkı saęlamaktır. En azından, umarım iřtahınızı körükler ve bu dikkat çekici ve akıcı konuya daha derinlemesine gitmenizi teřvik eder. Güncel kalmanız dileęiyle. Geliřmeler için bakınız:

<http://www.diplomacy.edu/capacity/IG> ve www.diplomacy.edu/ig.

Jovan Kurbalija

Diplo Foundation Müdürü
Cenevre İnternet Platformu Bařkanı, Kasım 2016

Bölüm-1

Giriş

İnternet yönetiřimi, her ne kadar dijital dünyanın özü-nü ele alıyor olsa da, yönetiřim, ikili dijital mantıkta olduđu gibi doğru/yanlıř ve iyi/kötü řeklinde ele alınamaz. Bunun yerine, İnternet yönetiřimi birçok incelik, anlam ve algı tonlarını gerektirir; bu yüzden İnternet yönetiřimi bir dizi seçenek ve uzlařıyı kapsayan analog bir yaklařım gerektirmektedir.

Bundan dolayı bu kitap, İnternet yönetiřimine iliřkin konularda kesin önermeler sunmaya çalışmamaktadır. Kitap daha çok, bu alandaki önemli konuların analizi, tartiřılması ve çözüme kavuřturulması için pratik bir çerçeve önerme amacı tařımaktadır.

GİRİŞ

İnternet yönetişimini çevreleyen tartışma, kavramın tanımı ile başlamaktadır. Söz konusu kavram yalnızca dilbilimsel akıl yürütme, farklı bakış açıları, yaklaşımlar ve beklentilerden ibaret değildir. Örneğin, telekomünikasyon uzmanları İnternet yönetişimine teknik altyapının geliştirilmesine yönelik prizmadan bakarlar. Bilgisayar uzmanları XML (Genişletilebilir İşaretleme Dili) veya Java gibi farklı standart ve uygulamaların geliştirilmesine odaklanırlar. İletişim uzmanları iletişimin kolaylaştırılması üzerine vurgu yaparlar. İnsan hakları aktivistleri İnternet yönetişimine ifade özgürlüğü, mahremiyet ve diğer temel insan hakları çerçevesinden bakarlar. Avukatlar yargı yetkisi ve ihtilaf çözümü üzerine yoğunlaşırlar. Dünyadaki siyasetçiler genellikle kendi seçmenleri arasında yankı uyandıran tekno-optimizm (daha çok bilgisayar=daha çok eğitim) ve tehditler (siber güvenlik, siber suç, çocuk koruma) gibi konular üzerine odaklanırlar. Diplomatlar ulusal çıkarların öne çıkarılması ve korunması ile ilgilenirler. İnternet yönetişimine yönelik potansiyel çelişen mesleki bakış açılarının listesi, bu şekilde sürüp uzayıp gitmektedir.

İnternet Yönetişimi ne anlama gelir?

Dünya Bilgi Toplumu Zirvesi (WSIS)¹ İnternet yönetişimine ilişkin olarak aşağıdaki geçerli tanımı yapmıştır:

İnternet yönetişimi hükümetler, özel sektör ve sivil toplumun İnternetin evrimini ve kullanımını şekillendiren, paylaşılan ilkeler, normlar, kurallar, karar alma usul ve programlarını geliştirmesi ve uygulamasıdır.²

Oldukça geniş yapılan bu geçerli tanım, iki temel kavramın farklı şekillerde yorumlanması sorununu çözmemektedir: “İnternet” ve “Yönetişim”

‘İ’nternet veya ‘i’nternet ve diplomatik işaretleşme

The Economist dergisi 2003 yılında İnternet sözcüğünü küçük “i” harfi ile yazmaya başladı. Yayın politikasındaki bu değişiklik İnternet’in artık büyük harfle yazılmasını gerektirecek kadar benzersiz ve özel olmaktan çıkıp, gündelik bir öge haline gelmesinden esinlenmişti. “İnternet” sözcüğü (t)elgraf, (t)elefon, (r)adyo ve (t)elevizyon ve benzeri diğer icatların dilsel kaderini takip etmişti.

İnternet/internet sözcüğünü büyük mü yoksa küçük (i) harfiyle yazılacağına yönelik belirsizlik, “İnternet” teriminin İnternet yönetişimine yönelik Uluslararası Telekomünikasyon Birliği (ITU) kararında normalde kullanıldığı şekilde büyük “İ” değil de küçük “i” ile kullanıldığında siyasi bir boyutun tanıtıldığı Antalya’da gerçekleştirilen ITU Konferansı’nda (Kasım, 2006) yeniden gündeme gelmiştir. İnternet yönetişiminden sorumlu ABD Büyükelçisi, David Gross, ITU’nun gerçekleştirdiği küçük harfle kullanımın, İnternetin ITU tarafından idare edilen diğer telekomünikasyon sistemleri ile aynı muameleyi görme niyetini işaret edebileceği yönündeki endişesini dile getirmiştir. Bazıları bunun ITU’nun İnternet yönetişimi konusunda daha belirgin bir rol oynama niyetine yönelik diplomatik bir belirteç olarak yorumlamıştır.³

İnternet

“İnternet” terimi küresel dijital gelişmelerin mevcut her türlü yönünü kapsamamaktadır. Diğer iki terim (Bilgi Toplumu ile Bilgi ve İletişim Teknolojileri) genellikle daha kapsayıcı şekilde ortaya konulmaktadır. Bu iki kavram mobil telefon hizmetleri gibi İnternet alanının dışında kalan alanları da kapsamaktadır. Ne var ki küresel iletişimin hızlı bir şekilde İnternet Protokolünün (IP) temel iletişim teknik standardı olarak kullanımına geçişi ile “İnternet” teriminin kullanımına yönelik tartışma büyümüştür. Hâlihazırda yaygın hale gelen İnternet, yalnızca kullanıcı sayısı açısından değil aynı zamanda, geleneksel telefon hizmetlerinin yerini alabilecek IP üzerinden ses iletimi (VoIP), IP tabanlı televizyon (IPTV) gibi zirve olarak adlandırılan ve giderek yaygınlaşan ve geleneksel telefon ve televizyon hizmetlerine karşı ciddi rakip olarak görülmeye başlayan hizmetler açısından da ile süratle genişlemeye devam etmektedir.

Yönetişim

İnternet yönetişimi ile ilgili tartışmada, “yönetişim” terimi ve onun muhtelif yorumlarında ihtilaf ortaya çıkmıştır. Yorumlardan birine göre, yönetişim (governance), devlet yönetimi (government) kelimesi ile eşanlamlıdır. Dünya Bilgi Toplumu Zirvesi’nin (WSIS) ilk süreçlerinde, ulusal delegasyonların çoğu bu ilk anlayışı benimsemiştir ki, bu da İnternet yönetişiminin hükümetlerin işi olması gerektiği ve konunun diğer aktörlerin, özellikle de devlet dışı aktörlerin sınırlı katılımı ile hükümetlerarası düzeyde ele alınmasına işaret ettiği anlayışına yol açmıştır.

İnternet yönetişimi teriminin bazı uluslararası kuruluşlar tarafından nasıl kullanıldığına bakarsak konuyla ilgili daha da fazla kafa karışıklığı olduğu görünür. Örneğin, Dünya Bankası tarafından devlet reformlarında şeffaflığın daha fazla olmasını, yolsuzluğun azaltılmasını, yönetimin verimliliğinin artırılmasını teşvik etmek maksadıyla ‘iyi yönetişim’ terimi kullanılmıştır.

Bu yorumlar “yönetişim” teriminin, devlet kurumu olmayanlar da dâhil herhangi bir kurumun işlerinin yönetişimini içeren kapsamlı anlamıyla çatışmaktadır. Bu, İnternetin ilk zamanlarından beri yönetildiği biçimi tanımladığı için İnternet toplumunun kabul ettiği bir yorum olmuştur.

Terminolojik karışıklık, “yönetişim” teriminin diğer dillere tercümesi ile daha da karmaşık bir hal almıştır. İspanyolca’da terim esasen kamu eylemleri veya hükümet anlamına gelmektedir (gestión pública, gestión del sector público, ve función de gobierno). Kamu eylemleri veya hükümet anlamı aynı zamanda Fransızca’da da kendisini göstermektedir (gestion des affaires publiques, e cacité de l’administration, qualité de l’administration, vemode de gouvernement). Portekizce de kamu sektörü ve hükümete atıfta bulunurken benzer bir yapı izlemektedir (gestão pública ve administração pública).

İnternet Yönetişiminin Evrimi

İlk Zamanlarda İnternet Yönetişimi (1970-1994)

İnternet bir hükümet projesi olarak başlamıştır. 1960’lı yılların sonlarına doğru, ABD hükümeti bilgisayarlar arasında dijital kaynakların paylaşımını kolaylaştırmayı amaçlayan Araştırma Projeleri Ajansı Bilgisayar Ağı (ARPANet)’nin geliştirilmesine mali destek sağlamıştır. 1970’li yılların ortalarında TCP/IP’nin (İleti Kontrol Protokolü/İnternet Protokolü) icadı ile bu ağ bugün İnternet olarak bildiğimiz hale evrilmiştir. İnternetin temel ilkelerinden birisi onun dağıtım yapısidir: veri paketleri geleneksel engelleri ve kontrol mekanizmalarını aşarak ağ boyunca farklı yönlerde gidebilmektedir. Bu teknolojik ilke, ilk aşamalarda İnterneti düzenlemeye benzer bir yaklaşım ile uyumlu olmuştur. 1986 yılında kurulan İnternet Mühendisliği Çalışma Grubu (IETF), işbirlikçi ve mutabakata dayalı karar verme süreci vasıtasıyla, çok geniş çapta paydaş, çalışmalara dâhil ederek İnterneti daha da geliştirme çabasına girişmiştir. Merkezi herhangi bir hükümet, merkezi bir planlama veya başka büyük bir plan olmamıştır.

Bu da pek çok insanın, İnternetin bir şekilde benzersiz bir şey olduğunu ve modern dünya siyasetine bir alternatif önerebileceğini düşünmesine yol açmıştır. Ünlü [Siber Mekânın Bağımsızlık Bildirgesi](#)’nde, Amerikalı siber liberteryen siyaset aktivisti John Perry Barlow şunları söylemiştir:

[İnternet] milletler üstü doğası gereği egemenlik karşıtıdır ve sizlerin [devletlerin] egemenliği bizim için geçerli değildir. Bizler bir şeyleri kendimiz çözmek zorundayız.⁴

Alan Adı Sistemi (DNS) Savaşı (1994-1998)

İnternet yönetişimine âdemi merkeziyetçi yaklaşım hükümetlerin ve özel sektörün küresel ağın öneminin farkına varmasıyla kısa süre içinde değişmeye başlamıştır. 1994 yılında, İnternetin kilit altyapısını idare eden ABD Ulusal Bilim Vakfı (NSF), DNS yönetiminde Ağ Çözümleri Şti. (NSI) adlı özel bir Amerikan şirketini taşeron olarak kullanma kararı almıştır. Bu durum İnternet toplumu tarafından hoş karşılanmayarak DNS savaşı adı verilen duruma yol açmıştır.

Bu “savaş” tabloya yeni oyuncular eklemiştir: uluslararası örgütler ve ulus devletler. Savaş 1998 yılında, ABD hükümeti ile yapılan sözleşme esasına göre temel İnternet teknik kaynaklarının koordinatörü olan İnternet Tahsisli Sayılar ve İsimler Kurumu (Internet Corporation for Assigned Names and Numbers-ICANN) adlı yeni bir örgütün kurulması ile son bulmuştur. ICANN günümüzde de İnternet yönetişi konusundaki pek çok tartışmanın odak noktası olmuştur.

Dünya Bilgi Toplumu Zirvesi (WSIS) (2003-2005)

Cenevre’de (2003) ve Tunus’ta (2005) düzenlenen WSIS resmi olarak İnternet yönetişi sorununu diplomatik gündemlere taşımıştır. Bir kaç Hazırlık Komitesi (PrepComs) ve bölgesel toplantılar ile öncülük edilen zirvenin Cenevre aşaması katılımcılar tarafından ileri sürülen Bilgi ve İletişim Teknolojisine (ICT) ilişkin bir dizi konu ile oldukça kapsamlı olmuştur. Esasında, ilk hazırlık ve bölgesel toplantılar esnasında, “İnternet yönetişi” terimi kullanılmamıştır.⁵ İnternet yönetişi WSIS sürecine, Cenevre zirvesi sonrasında WSIS müzakerelerinin kilit meselesi haline geldikten sonra, Şubat 2003’te gerçekleştirilen Batı Asya bölgesel toplantıları esnasında sunulmuştur.

Uzun süreli müzakereler ve son dakika düzenlemelerinin ardından, 2003 yılındaki WSIS Cenevre zirvesi WGIG’in kurulması konusunda mutabakata varmıştır. WGIG Tunus’ta gerçekleştirilen ikinci WSIS zirvesinde (Kasım 2005) gerçekleştirilen müzakerelere temel teşkil etmek üzere bir rapor⁶ hazırlamıştır. WSIS **Bilgi Toplumu İçin Tunus Gündemi**, WGIG tarafından önerilen bir tanımın benimsenmesi, İnternet yönetim meselelerinin listelenmesi ve İnternet yönetişi ile ilgili temel unsurlara ilişkin kamu politikaları konusunda tartışmalar için bir alan olarak işlev görmek üzere BM Genel Sekreteri tarafından resmi olarak önerilen çok paydaşlı bir yapı olan İnternet Yönetişim Forumu’nun (IGF) kurulması konusu da dâhil olmak üzere İnternet yönetişimine yönelik sorunu ayrıntılarıyla ele almıştır.⁷

2006 Yılındaki Gelişmeler

Tunus zirvesinden sonra, 2006 yılında üç temel gelişme ve olay İnternet yönetişi tartışmasına damgasını vurmuştur. Bunlardan ilki mevcut Mutabakat Anlaşması’nın (MoU) sona ermesi ve ICANN ile ABD Ticaret Bakanlığı arasında yeni bir anlaşmanın imzalanması olmuştur. Bazıları bu olayın ICANN ile ABD hükümeti arasındaki ilişkide değişiklik yaratabileceği ve ICANN’ın yeni bir uluslararası örgüt biçimi olabileceği beklentisine girmiştir. Ancak yeni Mutabakat Anlaşması ICANN ile ABD hükümeti arasındaki göbek bağına zayıflatırken, ICANN’ın statüsünün sonunda uluslararası bir hal alma ihtimalini de sürdürmüştür.

2006 yılında meydana gelen ikinci olay ise Atina’da gerçekleştirilen IGF olmuştur. Forum bu alanda gerçekleştirilen ilk forum olup, pek çok yönden çok taraflı diplomaside bir deney niteliği taşımıştır.

IGF, gerçekten çok paydaşlı bir yapıda oluşmuştur. Tüm taraflar (devletler, işletmeler, akademik ve teknik topluluklar ve sivil toplum) eşit temelde katılım sağlamışlardır. Forum ayrıca zamanda temel olaylar ve çalıştayları ile de ilginç bir örgütsel görüntü vermiştir. Gazeteciler tartışmalara başkanlık etmiş, bu yüzden IGF alışıldık BM toplantı formatından ayrılmıştır. Ancak bazı

eleştirmenler IGF'in nihai bir belge veya eylem planı formatında somut herhangi bir sonuca varmayan bir "söyleşi programından (talk show)" ibaret olduğunu öne sürmüşlerdir.

2006 yılında meydana gelen üçüncü gelişme ise Kasım ayında Türkiye'da Antalya'da gerçekleştirilen ITU Tam Yetkili Temsilciler Konferansı olmuştur. Bu konferansta ITU Genel Sekreteri olarak Dr. Hamadoun Touré seçilmiştir. Kendisi siber güvenlik ve kalkınma yardımları konuları üzerine daha fazla yoğunlaşılacağını bildirmiştir. Kendisinden ITU'nun İnternet yönetişimine yönelik yaklaşımlarına yeni yöntemler getirmesi beklenmiştir.

2007 Yılındaki Gelişmeler

ICANN ile ilgili tartışma (yetişkin içeriklerine yönelik) .xxx uzantılı alan adları üzerine odaklanarak, ICANN'ın yalnızca teknik sorunlarla mı yoksa kamu politikasına ilişkin konularla da mı ilgilenmesi gerektiği de dahil olmak üzere pek çok yönetim hususuna yönelik tartışmaları yeniden gündeme getirmiştir.⁸ Bu çerçevede ABD ve diğer hükümetler tarafından (.xxx uzantılı alan adları ile ilgili olarak) yapılan müdahaleler, ulusal hükümetlerin ICANN müzakerelerine nasıl dahil olması gerektiği sorusunu gündeme getirmiştir.

Kasım ayında Rio de Janerio'da düzenlenen ikinci IGF'deki temel gelişme kritik İnternet kaynaklarını (isimler ve sayılar) IGF'in gündemine eklemek olmuştur.

2008 Yılındaki Gelişmeler

2008 yılının, diğer politika alanları kadar İnternet yönetişimi alanını da etkilemeyi sürdüren en önemli gelişmesi Barack Obama'nın ABD Başkanı olarak seçilmesidir. Başkanlık seçimi kampanyasında, Obama İnternet ve Web 2.0 araçlarını yoğun şekilde kullanmıştır. Öyle ki bazıları başarısının sebeplerinden birinin bu olduğunu öne sürmektedir. Başkanın danışmanları arasında, Google'ın CEO'su da dahil olmak üzere İnternet sektöründen gelen pek çok kişi bulunmaktaydı. Başkan Obama, teknolojik farkındalığının yanı sıra ICANN'ın uluslararası hale getirilmesi ve İnternet yönetişimi rejiminin geliştirilmesi konusundaki tartışmaları etkilemesi muhtemel olan çok yönlülüğü desteklemiştir.

2008 yılında, ağ tarafsızlığı⁹ İnternet yönetişimine yönelik en önemli meselelerden birisi olarak ortaya çıkmıştır. Konu öncelikle ABD'de iki ana muhalefet bloğu arasında tartışılmıştır. Hatta Başkan Obama tarafından desteklenen ABD başkanlık kampanyasında öne çıkmıştır. Ağ tarafsızlığı esasen Google, Yahoo! ve Facebook gibi şirketlerin dahil olduğu bir kısım İnternet endüstrisi olarak bilinen kesim tarafından da desteklenmiştir. İnternet mimarisinde ağ tarafsızlığındaki bir çatlak ile tetiklenecek bir değişim bu kesimin yaptıkları işi tehlikeye atabilecektir. Diğer tarafta ise Verizon ve AT&T gibi telekomünikasyon şirketleri, İnternet hizmet sağlayıcıları (ISP) ve multimedya sektörü yer almaktadır. Farklı sebeplerden ötürü bu kesim İnternette gezinen paketlerde bir çeşit farklılaşma görmek istemektedirler.

Ağ tarafsızlığı konusunda daha fazla tartışma için 2. Bölüme bakınız.

Diğer büyük gelişme ise Facebook ve benzeri sosyal ağların hızlı büyümesi olmuştur. İş İnternet yönetişimine gelince, Web 2.0 araçlarının kullanımının artması sosyal medya platformlarında özel hayatın gizliliği ve kişisel verilerin korunması konularını gündeme getirmiştir.

2009 Yılındaki Gelişmeler

2009 yılının ilk bölümünde Washington Kemerî'nin, Başkan Obama'nın İnternete ilişkin politikasının olası sonuçları ve ileriye yönelik gidişatını anlamaya çalıştığı görülmüştür. Obama'nın İnternetle alakalı kilit pozisyonlara yaptığı atamalar beraberinde büyük herhangi bir sürpriz getirmemiştir. Atanan kişiler açık bir İnternet için Başkanın desteğini takip etmişlerdir. Başkanın ekibi aynı zamanda ağ tarafsızlığı ilkesinin seçim kampanyası esnasında vermiş olduğu vaatler doğrultusunda uygulanması için uğraşmışlardır.

2009 yılının en önemli olayı ise ICANN'ın daha bağımsız bir örgüt olmasını sağlayacak olan ICANN ile ABD Ticaret Bakanlığı arasında Taahhütlerin Onaylanması olmuştur. Bu adım İnternet yönetişimi konusundaki bir sorunu (ABD'nin ICANN üzerindeki denetim rolünü) bir adım öteye taşıırken, ICANN'ın uluslararası konumu ve ICANN faaliyetlerinin daha fazla denetlenmesi gibi yeni pek çok meseleyi gündeme getirmiştir. Taahhütlerin Onaylanması ilkelere ortaya koymuş ancak ileriki yıllarda değinilecek pek çok meseleyi de bir kenara bırakmıştır.

2009 yılının Kasım ayında Mısır'da Şarm El-Şeyh'de dördüncü İnternet Yönetişim Formu düzenlenmiştir. Forumun ana konusu, Forumun yetkisinin 2010 yılında gözden geçirilmesi ışığında Forumun geleceği olmuştur. Taraflar yapmış oldukları sunularda Forumun geleceği konusunda çok çeşitli görüşlere yer vermişlerdir. Pek çoğu Forumun sürdürülmesini desteklese de, gelecekteki Forumun nasıl örgütlenmesi gerektiği konusunda büyük görüş farklılıkları yaşanmıştır. Çin ve gelişmekte olan pek çok ülke hükümetlerin rollerini daha önemli hale getireceği varsayımıyla Forumun BM sistemi içerisine daha güçlü bir şekilde bağlanması gerektiğini ileri sürmüştür. ABD, gelişmekte olan ülkelerin pek çoğu, özel sektör ve sivil toplum ise mevcut Forum modelinin korunması gerektiğini öne sürmüşlerdir.

2010 Yılındaki Gelişmeler

2010 yılındaki en önemli gelişme, Facebook gibi sosyal medya platformlarındaki kullanıcıların gizliliğinin korunması konusu da dâhil olmak üzere, hızla büyüyen sosyal medyanın İnternet yönetişimi tartışması üzerindeki etkisi olmuştur. 2010 yılında İnternet jeopolitiği konusundaki esas gelişme ise ABD Dış İşleri Bakanı Hilary Clinton'ın, bilhassa Çin ile alakalı olarak, İnternet ortamında ifade özgürlüğü üzerine yapmış olduğu konuşma olmuştur.¹⁰ Google ve Çinli yetkililer Çin'deki Google arama motoruna sınırlı erişim konusunda anlaşmazlığa düşmüşlerdir. Anlaşmazlık Google'ın arama faaliyetlerinin Çin'de kapatılmasına yol açmıştır.

ICANN dünyasında iki önemli gelişme yaşanmıştır. Bunlardan ilki Arapça ve Çince için AS-CII olmayan karakterleri içerebilen alan adlarının çıkarılması olmuştur. ICANN Latin kökenli olmayan diğer dillerdeki üst-seviye alan adı sorununu çözerek İnternet DNS'inin dağılması riskini azaltmıştır. İkincisi ise ICANN'ın .xxx uzantılı alan adını (yetişkin içeriği) onaylaması

olmuştur. Bu karar doğrultusunda ICANN resmi olarak İnternet konusunda kamu politikası ile yakından alakalı bir kararı kabul ederek Rubicon ile resmen ters düşmüştür. Daha öncesinde ICANN en azından resmi olarak yalnızca teknik kararların alınması alanı içerisinde kalmaya çalışmıştır.

IGF'nin gözden geçirilme süreci BM Kalkınma İçin Bilim ve Teknoloji Komisyonu'nun Forumu (UNCSTD) beş yıl daha organizasyon ve yapısında yalnızca küçük değişiklikler ile sürdürülmesini öneren kararı ile başlamıştır. 2010 Temmuz ayında, BM Ekonomik ve Sosyal Konseyi (UNECOSOC) bu kararı kabul etmiş ve IGF'nin sürdürülmesine yönelik nihai karar 2010 yılının sonbaharında BM Genel Kurulu'nda alınmıştır.

2011 Yılındaki Gelişmeler

2011 yılında genel anlamdaki en büyük gelişme İnternet yönetişimi konusunun küresel siyasi gündemde yükselişi olmuştur. İnternet yönetişimi, iklim değişikliği, göç ve gıda güvenliği gibi diğer diplomatik meselelerle daha yakın bir ilişki içerisine girmiştir. İnternetin siyasetle güçlenen ilişkisinin diğer bir sonucu da İnternet yönetişimi meselelerinin ulusal kapsamında zamanla (IT, Telekom gibi) teknoloji konularından (diplomasi, hükümet kabineleri gibi) siyasi konularına doğru kayma yaşanmasıdır. Bunun yanı sıra, küresel ana akım medya (örneğin: The Economist, IHT, Al Jazeera, BBC) artık İnternet yönetişimine yönelik gelişmeleri her zamankinden çok daha yakından takip eder olmuştur.

İnternet yönetişimi Arap Baharından etkilenmiştir. İnternet'in Arap Baharı olayı üzerindeki etkisine yönelik (küçük etkilerden çok önemli etkilere kadar) oldukça farklı görüşler yer alsa da, yarattığı şu sonuç kesindir: sosyal medya günümüz siyasi hayatında artık belirleyici olabilen bir araç olarak algılanmaktadır. İnternet -ve yönetişimi- 2011 yılında dünya genelinde muhtelif şekillerde siyasi radarlara girmiştir.

27 Ocak'ta Mısırlı yetkililer, gösterileri durdurma umuduyla İnterneti kestiler. Bu durum hükümet emriyle ülke çapında İnternet kesintisinin ilk örneği olmuştur. Daha öncesinde, (eski Yugoslavya, Irak gibi) askeri çatışmalar esnasında dahi İnternet iletişimi asla tam olarak koparılmamıştır.

Hilary Clinton'un 2010 Şubat ayında yapmış olduğu konuşma ile İnternet üzerindeki ifade özgürlüğüne yönelik olarak başlatılan girişimi 2011 yılında hız kazanmıştır. Bu hususta iki temel konferans gerçekleşmiştir: İnsan Hakları ve İnternet Üzerine Viyana Konferansı ve İnternet ve Özgürlük üzerine Lahey Konferansı.

2011 yılında ICANN aşağıdaki temel gelişmeler ile kendini motive eden şeyleri gözden geçirmeye devam etmiştir:

- Yönetim reformunun uygulamaya konulması.
- Yeni jenerik üst düzey alan adlarının (gTLDs) tanıtımına yönelik nihai politika hazırlıkları.
- Yeni bir yönetici (CEO) arayışı.
-

2011 yılı aynı zamanda Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Avrupa Konseyi, AB, Brezilya ve diğer oyuncular tarafından önerilen çok sayıda İnternet yönetişimi ilkesiyle dik-kati çekmiştir. Bu ilkelere yönelik sayısız kesişim küresel bir İnternet bildirgesinin veya İnternet yönetişiminin gelişimine çerçeve teşkil edecek benzer bir dokümanın gelecekteki önsözü için bir başlangıç noktası gibi telakki edilmiştir.

2012 Yılındaki Gelişmeler

Önümüzdeki yıllar için önemli sonuçlar doğurması beklenen iki önemli olay 2012 yılının gün-demini belirlemiştir: ICANN'daki lider değişimi ve ITU'nun [Uluslararası Telekomünikasyon Düzenlemelerinin](#) (ITR'lerin) gözden geçirilmesi.

ICANN, yeni üst düzey alan adlarının (gTLD'lerin) piyasaya sürülmesiyle bir önceki yıla göre önemli gelişmeler yaşamıştır. Kayıt süreciyle ilgili (yazılımla ilgili küçük teknik problemler, politika sürecine ilişkin tartışmalar gibi) bazı sorunlara rağmen, yeni gTLD'ler için 1900'den fazla başvuru alınmış ve sonuçta 2014'te başlayarak hangi gTLD'lerin uzantı olarak kabul edile-ceğine karar verecek bir değerlendirme sürecine sokulmuştur. Dahası, yeni CEO Fadi Chehadé ICANN'ın politika süreçlerinin çok taraflı idaresine yeni bir yaklaşım getirmiştir. ICANN 45 toplantısında sivil topluma yaptığı konuşmasında, Chehadé ICANN'de, sorumlu çok taraflılı-ğın geliştirilmesi, sorunların samimi şekilde tanınması, aktif dinleme, empatik rehberlik, uzlaş-ma arayışı gibi konularda gelişmelere ilişkin bazı vaatlerin altını çizmiştir.

Uluslararası Telekomünikasyon Konferansı (WCIT), Aralık 2012'de Dubai'de 1988'den bu yana ilk kez ITR'leri değiştirmek üzere bir araya geldi; yıl boyunca ilgi çekti ve yeni bir düzenle-melerin İnternet'in geleceği üzerindeki etkisi ile ilgili kaygıları dile getirdi ve tartışmaya açtı. Yo-rucu bir iki hafta süren konferansın sonunda, müzakereler bir çıkmaz ile sona erdi: katılımcılar değiştirilen metin üzerinde bir uzlaşmaya varamadılar ve tartışma yaklaşmakta olan toplantılar için açık bırakıldı. Çekişmeli nokta, ITU'nun İnternet yönetişimindeki rolünü güçlendirmeye yönelik bağlayıcı olmayan bir karardı ve bu, katılımcı ülkeleri mevcut çok taraflı modeli destek-leyen batılı ülkeler ile Çin, Rusya ve Arap ülkeleri gibi hükümetlerarası bir modelden yana olan ve kararı destekleyen ülkeler olmak üzere iki blokta kutuplaştırdı.

İnternet kullanıcılarının mobilizasyonu ve protestolarının ABD'de Çevrimiçi Korsanlığı Dur-durma Yasası (SOPA) ve uluslararası Sahteciliğe Karşı Ticaret Anlaşması (ACTA) gibi düzen-lemelerin uygulanmasının kullanıcıların meşru haklarını etkileyebileceği düşüncesiyle bu dü-zenlemeleri engelleme çabaları ile birlikte, fikri mülkiyet hakları (IPR) alanında kayda değer gelişmeler de yaşanmıştır.

2013 Yılındaki Gelişmeler

Küresel dijital politikadaki ana gelişme, ABD Ulusal Güvenlik Ajansı (NSA) ve diğer ajanslar tarafından yürütülen çeşitli gözetim programlarının Snowden tarafından ifşası idi. Snowden'in ifşaları, küresel kamuoyunun ilgisini İnternetin nasıl yönetildine yöneltti. ilgilendi. Asıl odak, mahremiyet ve veri koruma hakkı sorunu haline geldi.

Mahremiyetin korunması sorunu Birleşmiş Millet Genel Kurulu (UNGA) süresince birçok lider tarafından dile getirildi. UNGA kararı, çevrimiçi gizlilik konusunda yeni bir politika süreci başlattı. Mesele 2014 yılında BM İnsan Hakları Konseyi'nde (UNHRC) daha ayrıntılı olarak ele alınacaktı.

Ekim 2013'te Brezilya Devlet Başkanı Dilma Rousseff ve ICANN'ın Başkanı Fadi Chehadé NETmundial sürecini başlattı. İnternet yönetişimi sayısız akademik konferansta ve dünya genelinde düşünce kuruluşlarının araştırma faaliyetlerinde odaklandı.

2014 Yılındaki Gelişmeler

2014 yılı, ABD Başkanı Obama'nın NSA gözetimi konusundaki konuşmasıyla başladı. "siber saldırı" terimini, siber güvenliği (terörizmden daha fazla olmak üzere) güvenlik gündeminin ön sıralarına yerleştirerek tekrar tekrar kullandı.

14 Mart'ta, ABD Ticaret Bakanlığı'na bağlı Ulusal Telekomünikasyon ve Enformasyon İdaresi (NTIA), temel alan adı işlevleri üzerindeki yöneticilik rolünü küresel çok paydaşlı topluluğa geçirmek niyetinde olduğunu açıkladı. Bu noktada, NTIA, diğer kritik parametrelerin yanı sıra, İnternet Atanmış Numaralar Kurumu'nun (IANA) küresel IP adresleri ve alan adlarının kayıtlarının tutulmasını da içeren işlevlerinin performansını denetlemiştir.

NTIA ayrıca (küresel bir İnternet adres defteri olan) kök alan dosyasındaki değişikliklere izin vererek bir emniyet sübubu oluşturdu. Bunun ilan edilmesi, danışma ve önerilerin konsolidasyonu için 2015 yılında tamamlanması planlanan fakat daha sonra bir yıl uzayan uzun bir süreci tetiklemiştir. Aynı zamanda, ICANN içinde hesap verebilirlik mekanizmalarının konsolidasyonun hedefleyen bir süreç de başlatılmıştır.

İkisi ICANN ile ilgili olmak üzere üç tartışma forumu ortaya çıkmıştır:

- Muhtelif destek gruplarını birbirine bağlamak ve tartışma özetlerini diğer forumlara, özellikle de NETmundial sürecine taşımak için ICANN tarafından /1net (çevrimiçi) platform başlatılmıştır. /1net ve Brezilya İnternet Yönlendirme Komitesi (CGI.br) tarafından ortaklaşa düzenlenen NETmundial konferansı 23 ve 24 Nisan tarihlerinde São Paulo'da gerçekleşmiştir. Konferans bir dizi İnternet yönetişimi ilkesinin yanı sıra İnternet yönetişimi ekosisteminin gelecekteki evrimi için bir yol haritasını da içeren [Çok Paydaşlı NETmundial Bildirimi](#) ile sonuçlanmıştır.
- Küresel İnternet İşbirliği ve Yönetişim Mekanizmaları (GICGM) konusunda Sunnyslands'daki Annenberg Retreat'in yardımlarıyla, ICANN ve Dünya Ekonomik Forumu (WEF) ortaklığıyla Üst Düzey Panel oluşturulmuştur. Panel, işbirlikçi ve adem-i merkezi bir İnternet yönetişimi ekosisteminin geliştirilmesi için bir dizi öneriyi ortaya koyan, [İşbirliğine Dayalı, Adem-i Merkezi bir İnternet Yönetişimi Ekosistemine Doğru](#) adlı bir rapor ortaya koymuştur.
- Kanada Uluslararası Yönetişim İnovasyon Merkezi ve İngiltere merkezli düşünce kuruluşu Chatham House tarafından, İnternet yönetişiminin geleceğine ilişkin stratejik bir vizyon geliştirmek amacıyla "İnternet Yönetişimi Komisyonu" kurulmuştur.

Avrupa Birliği Adalet Divanı (CJEU) 3 Mayıs'ta bir bireyin kendi adıyla görüntülenene araştırma sonuçlarının birey tarafından bir talepte bulunulması halinde “günü geçmiş”, “aşırı” ve “ilgisiz” kişisel verilere yönelik bağlantıların Google tarafından silinmesini öngören ‘unutulma hakkı’nı tanımıştır.

2015 Yılındaki Gelişmeler

Yıl boyunca, IANA yönetim geçişi ve ICANN’ın sorumluluğu, sürecin Eylül 2016’ya kadar uzadığı süre boyunca odakta kalmıştır. Siber güvenlik, hem güvenlik ihlalleri hem de politikaya tepkiler bakımından gündemin üst sıralarında kalmaya devam etmiştir. 2013’ün başlarında, mevcut uluslararası hukukun devletler tarafından Bilgi ve İletişim Teknolojileri kullanımı için geçerli olduğuna karar verdikten sonra, BM Uluslararası Güvenlik Bağlamında Bilgi ve İletişim Alanındaki Gelişmelerle ilgili Hükümet Uzmanları Grubu (UN GGE) kritik altyapılara veya Bilgisayar Acil Durum Müdahale Ekiplerine (CERT) saldırı yapmamak ve topraklarında siber saldırı ve siber suçları soruşturmada diğer uluslara yardım etmek de dahil olmak üzere bazı normlar üzerinde anlaşmaya varmıştır.

Temmuz ayında, sürdürülebilir kalkınma hedefleri (SDGs) sürecinin bir parçası olarak, BM, bilim, teknoloji ve inovasyon konusunda bir BM kurumlar arası görev takımını kapsayan çok paydaşlı bir forum; ve yeni bir çevrimiçi ‘haritalama’ platformunu içeren yeni bir [Teknoloji Ko-laylaştırma Mekanizması](#)¹¹ kurmuştur. UNHRC tartışmalarının ardından, gizlilik hakkı konusunda özel bir mekanizma üzerinde anlaşılmış ve ilk Özel Gizlilik Raporörü (Profesör Joseph Cannataci) 3 Temmuz’da atanmıştır.

2015 yazı ayrıca WSIS+10’u gözden geçirme sürecinin başlamasıyla dikkat çekti ve Aralık ayında WSIS sonuçlarının uygulanmasının genel olarak gözden geçirilmesine ilişkin olarak Genel Kurulun Üst Düzey Toplantısı ile sona erdi. Burada kabul edilen sonuç belgesi, IGF’nin görevini bir on yıl daha yenilemiş ve tarafların 2005 Tunus Gündeminde yer alan rol ve sorumluluklarını pekiştirerek gelecek on yıldaki gelişme yönünü vurgulamıştır.

ICANN topluluğu içinde, IANA yönetim geçişi ve ICANN’ın hesap verebilirliği önerilerinin geliştirilmesi çalışmaları devam etmiştir.

2016 Yılındaki Gelişmeler

2016 yılı, temel bir soruyu gündeme getiren iki raporla başladı: Fırsatları nasıl en üst düzeye çıkarır ve İnternet’in getirdiği riskleri en aza indiririz? Dünya Bankası’nın [Dünya Kalkınma Raporu 2016: Dijital Paylar](#),¹² İnternet’in toplum için otomatik olarak fayda sağlamayacağını ileri sürmüştür. İnternetin toplum üzerinde olumlu bir etkisi olmasını sağlamak için politika, eğitim ve çok daha fazlasına ihtiyaç vardır. WEF, küresel İnternet için var olan riskleri (teknik, devlet ve ticari parçalanma şeklinde) ortaya koyan İnternet parçalara ayrılması hakkında daha dikkatli bir rapor yayınlamıştır.¹³

Apple ile ABD Federal Soruşturma Bürosu (FBI) arasındaki bir mahkemenin Aralık 2015’te San Bernardino, California’da 14 insanı öldüren teröristlerden birine ait bir iPhone telefonun

çözümlemesi için Apple firmasının FBI'a yardım etmesini öngeren bir karar çıkartmasıyla başlayan ihtilaf 2016 yılında birkaç ay boyunca manşetlerde kaldı. Tartışma, dijital dünyada güvenlik ve insan hakları dengeleme konusundaki eski soruyu tekrar gündeme getirdi. Davanın (ABD hükümetinin, telefonun devreye girmesi için üçüncü bir tarafın yardımından yararlandığını ileri sürmesi neticesinde) düşmesine rağmen, şifreleme, mahremiyet ve güvenlik ile ilgili konular yıl boyunca odakta kalmaya devam etti.

Haziran 2016'da, İnternet Yönetişimi Küresel Komisyonu, politika yapıcılara, özel sektöre, teknik topluluğa ve diğer paydaşlara sağlıklı bir İnternet'in muhafaza edilmesine ilişkin bir dizi öneri sunan **Tek İnternet** raporunu yayınladı. Rapor güvenli, güvenli, açık ve korunaklı bir İnternetin teşviki; dijital vatandaşların insan haklarının güvence altına alınması; özel sektörün sorumluluklarının belirlenmesi; İnternet'in çekirdek altyapısının istikrarını ve esnekliğini güvence altına almak; ve çok paydaşlı İnternet yönetişiminin iyileştirilmesi gibi hususları ele almaktadır.¹⁴

ICANN tarafında, yılın ilk yarısına ABD hükümetine IANA yönetimi geçiş önerisi ve ICANN'ın hesap verebilirliği teklifi sunulması damgasını vurmuştur. İki teklifi inceledikten sonra, NTIA, Ağustos 2016'da, önerilerin Mart 2014'te açıklanan kriterleri karşıladıklarını kabul etmiştir. Bu nedenle, ICANN, iki teklifin hükümlerini, özellikle de ICANN'ın bir alt kuruluşu olarak IANA işlevlerinin yerine getirilmesi ile görevli olacak Kamu Teknik Tanımlayıcılarının (PTI) oluşturulmasını, ve ICANN kararnamesinde ICANN'ı (personel ve Kurul açısından) eylemleri bakımından hesapverebilir hale getirmek için topluluğa daha fazla yetki veren bir dizi hükümün dahil edilmesini sağlamak suretiyle ICANN topluluğunun güçlendirilmesi görevini üstlenmiştir. 1 Ekim'de, ABD hükümeti ile ICANN arasındaki IANA işlevine ilişkin sözleşme IANA yönetiminin işlevlerinin küresel İnternet topluluğuna geçişine izin vererek sona ermiştir.

Önekler: e- / sanal / siber / dijital / net

e- / virtual / cyber / digital / net önekleri çeşitli ICT / İnternet gelişmelerini tanımlamak için kullanılır. Bunlar tipik olarak birbirlerinin yerine kullanılır. Her örnek bir İnternet fenomenini açıklar.

Yine de, e-'yi ticaret, siber'i suç ve güvenlik, dijital'i kalkınma dağılımları, sanal'ı Bitcoin gibi para birimleri için kullanma eğilimimiz mevcuttur. Kullanım şekilleri ortaya çıkmaya başlamıştır. Günlük dilimizde e- / sanal / siber / dijital / net ön eklerinin seçimi sıradan iken, İnternet politikasında ön eklerin kullanımı daha fazla anlam ve ilişki içermeye başlamıştır.

Bu terimlerin etimolojisine ve bunların İnternet politikasında nasıl kullanıldığına hızlıca bakalım.

'Siber'in etimolojisi, "egemen" in Antik Yunandaki anlamına dayanır. Siber günümüze Norbert Wiener'in bilgiyle çalışmayı ele alan *Cybernetics* adlı kitabı aracılığıyla gelmiştir.¹⁵ 1984 yılında, William Gibson bilim kurgu romanı *Neuromancer*'da¹⁶ siber uzay kelimesini kullanmıştır. "Siber" öneki kullanımındaki gelişme, İnternet'in gelişmesine paraleldir. 1990'ların sonlarında, İnternet ile ilgili neredeyse her şey "siber" ile ilişkilendirilmiştir: siber topluluk, siber kanun, siber seks, siber suç, siber kültür, siber... İnternette bir şeyi isimlendirdiyseniz ve "siber"iniz olmuş demektir. 2000'li yılların başlarında, siber kelimesinin geniş kullanımı giderek ortadan kalktı, sadece güvenlik terminolojisinde varlığını sürdürdü.

Siber kelimesi, 2001 Avrupa Konseyi Siber Suçlar Sözleşmesini adlandırmak için kullanılmıştır. Bu sözleşme hala İnternet güvenliği alanındaki tek uluslararası sözleşmedir. Bugün ABD'nin Siber Uzay Stratejisi, ITU'nun Küresel Siber Güvenlik Gündemi, Kuzey Atlantik Paketi'nin (NATO) Siber Savunma Politikası, Estonya'nın Siber Savunma Mükemmeliyet Merkezi gibi kullanımlar bulunmaktadır.

Cyberpunk yazarı ve Wired köşe yazarı Bruce Sterling şunları söylemiştir:

Askerin neden “siber” dediğini biliyorum - bunun nedeni, “siber uzaydan” oluşan bir “muharabe alanını” savunma metaforunun, belirli yüklenicilerin Pentagon hibelerini almasını kolaylaştırmasıdır. Eğer “siber uzayı”, “ağlar, teller, tüpler ve kablolar” ardışık paradigmasıyla tanımlarsanız, NSA elli yıllığına buna sahip olur ve silahlı kuvvetlerin söyleyecek tek sözü bile kalmaz.¹⁷

‘E’, “elektronik” kelimesinin kısaltmasıdır. İnternetin ilk ticarileştirilmesinin bir tanımı olarak olarak e-ticaretin kullanımıyla ilk ve en önemli kullanım etkisi ortaya çıkmıştır. AB'nin Lizbon Gündemi'nde (2000), e- en sık kullanılan örnek idi. E- öneki ayrıca, WSIS deklarasyonlarında ana örnek olmuştur (Cenevre 2003; Tunus 2005). WSIS'in takip uygulaması, e-devlet, e-ticaret, e-öğrenme, e-sağlık, e-istihdam, e-tarım ve e-bilimi içeren eylem planlarında merkezde yer almıştır. Bununla birlikte, e- öneki eskisi kadar kullanılmamaktadır. AB bile son zamanlarda e- önekinin kullanılmaktan giderek uzaklaşmıştır.

Bugün AB, Dijital Tek Pazar Stratejisi'nin¹⁸ uygulanmasına çalışmaktadır. Dijital, İnternet dünyasının temelini oluşturan iki sayı olan “1” ve “0” anlamına gelir. Sonuçta, tüm yazılım programları onlarla başlar. Geçmişte, dijital, dijital uçurumu temsil etmek amacıyla çoğunlukla kalkınma çevrelerince kullanılmıştır. Son birkaç yıl boyunca, dijital İnternet dilsel alanını fethetmeye başlamıştır. İnternetin temel öneki olarak kalması muhtemel görünmektedir. Avrupa Komisyonu Başkanı Jean - Claude Juncker, Avrupa Parlamentosu'ndaki ilk konuşmasında “dijital” ön ekini beş yıllık görev süresi için politika planını sunarken 10 kez kullanmıştır. AB'ye ek olarak, Büyük Britanya artık dijital diplomasiye sahiptir ve giderek artan sayıda diplomatik misyon, dijital meseleler için, genellikle bu meseleleri derinlemesine bilen, özel kişiler bulundurmaktadır.

Sanal öneki, İnternet'in maddi olmayan doğası ile ilgilidir. Sanal öneki, hem maddi olmayan hem de potansiyel olarak var olmayan belirsizlik taşımaktadır. Sanal gerçeklik, hem somut olmayan bir gerçeklik (hem dokunulmaz bir şey) hem de var olmayan bir gerçeklik (sahte bir gerçeklik) olabilir. Akademisyenler ve İnternet öncüleri, sanal önekinin İnternetin orijinallliğini ve cesur yeni bir dünya'nın ortaya çıkmasını vurgulamak kullanmışlardır. Sanal öneki, belirsiz anlamı nedeniyle, nadiren politika dilinde ve uluslararası belgelerde yer almaktadır.

Bugün önek hakimiyeti savaşında ateşkes görünmektedir. Her önek, örneğin 1990'ların sonlarında siber önekinin sahip olduğu üstün konumu koruyamadan kendi sınırları içerisinde kalmaktadır. Günümüzde siber öneki güvenlik konularındaki hakimiyetini korumaktadır. E- öneki ise hala iş için tercih edilen bir önektir. Dijital öneki, kalkınma sektörünün kullanımından devlet sektörü tarafından daha geniş kullanım alanına doğru gelişti. Sanal öneki ise neredeyse terk edilmiştir.

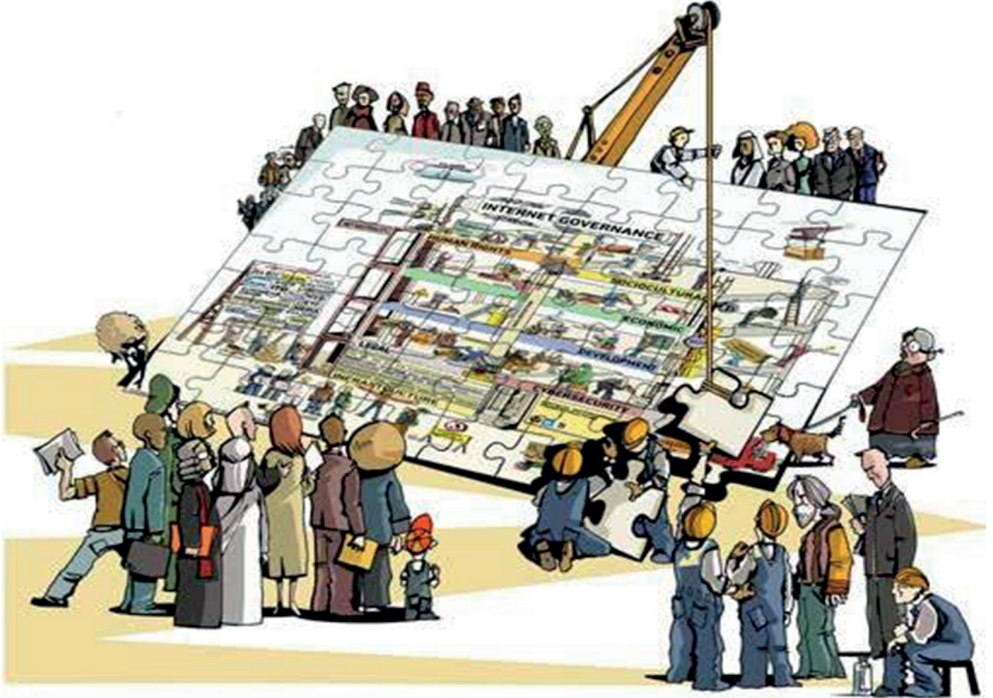
İnternet Yönetişimi Bilişsel Araç Kiti

Tersinin yanlış olduğu gün gibi ortada olan yüzeysel doğruların aksine, derin doğrular tersinin de doğru olması ile ayrılır.

Niels Bohr, Atom Fizikçisi (1885–1962)

İnternet Yönetişimi Bilişsel Araç Kiti, politika tartışmalarını geliştirme ve anlamaya yönelik bir araç setidir. Araç setinin temeli, neden-sonuç ilişkilerinin algılanışı, muhakeme şekilleri, değerler, terminoloji ve jargonu içerisine alan referans bir çerçevedir. Belirli meselelerin nasıl kapsama alınacağı ve ne gibi adımlar atılacağını şekillendirmektedir.

Pek çok durumda ortak bir referans çerçeve, belirli mesleki (örneğin diplomatlar, akademisyenler, yazılım geliştiriciler gibi aynı mesleğe mensup insanlar tarafından paylaşılan bilgi ve davranış biçimleri olan) kültürden etkilenmektedir. Bu tarz bir çerçevenin var oluşu genellikle daha iyi bir iletişim ve anlayışı kolaylaştırmaya yardımcı olmaktadır. Aynı zamanda mesleki alanı korumak ve dışardan gelecek etkileri engellemek için de kullanılabilir. Amerikan dilbilimci Jeffrey Mirel'den alıntı yapacak olursak "Her türlü mesleki dil bir özel alan dilidir".¹⁹



Şekil 1. İnternet yönetişimi bulmacası

İnternet yönetim rejimi karmaşık bir rejimdir zira pek çok konu, aktör, mekanizma, prosedür ve aracı bünyesinde bulundurmaktadır. Alman ressam MC Escher'den esinlenilen Şekil 1 İnternet yönetimiyle ilgili paradoksal bakış açılarının birkısını göstermektedir.

Araç takımı, politika geliştirmeyi belirli bir nedene bağlama konusunda karşılaşılan zorluklarla karakterize, sözde kötü bir politika alanı olarak adlandırılan İnternet yönetiminin doğasını yansıtmaktadır. Pek çok durumda her sorun bazen kısır döngüler yaratarak diğer bir sorunun belirtisi olmaktadır. Doğrusal, tek nedenli bilişsel yaklaşımlar ve/veya düşünceler İnternet yönetimi alanında sınırlı kullanıma sahiptir. İnternet yönetimi bir tutarlılık, çalışmemezlik ve bağdaşıklık korsesi içerisinde sıkıştırılmak için fazla karmaşıktır. Esneklik ve beklenmeyene karşı açık ve hazırlıklı olma İnternetin iyi bir yönü olarak düşünülmelidir.²⁰

İnternet yönetiminin süreci gibi araç kiti de sürekli değişmektedir. Yaklaşımlar, modeller ve analogiler, politika sürecindeki mevcut geçerliliklerine bağlı olarak ortaya çıkmakta ve ortadan kaybolmaktadır. İnternet yönetimi tartışmasında belirli politika anlatımlarını desteklemektedirler.

Politika yaklaşımları

İnternet Yönetimi Bilişsel Araç Kiti'nin ilk bölümünde, İnternet yönetim aktörlerinin ana konumlarına dayanak oluşturan bir dizi politika yaklaşım açıklanmaktadır. Bu politika yaklaşımları ayrıca müzakere konumlarının ve politika tartışmalarının çerçevesini açıklamaktadır.

Geniş yaklaşıma karşı dar yaklaşım

Dar kapsamlı yaklaşım İnternet altyapısının (DNS, IP adresleri ve kök sunucular) ve ICANN'ın bu alanda kilit bir aktör olarak konumu üzerine yoğunlaşmaktadır. Geniş kapsamlı yaklaşıma göre İnternet yönetimine yönelik müzakereler altyapısal konuların ötesine geçmeli ve yasal, ekonomik, gelişimsel ve sosyokültürel meselelere değinmelidir. Bu ikinci yaklaşım WGIG raporunda ve Bilgi Toplumu için Tunus Gündeminde kabul edilmiştir. Aynı zamanda IGF mimarisinin altında yatan ilke olarak kullanılmaktadır.

Bununla birlikte, siber güvenlik ve e-ticareti, İnternet yönetiminden ayrı politika alanları olarak görme eğilimi mevcuttur. Örneğin, 2015 WSIS + 10 inceleme belgesi²¹, farklı bölümlerde İnternet yönetimi ve siber güvenlik konularını ele almaktadır. Dijital politika tartışmalarının çerçevelenmesi, basit akademik bilginin epeyce ötesindedir. Politika silolarında (örneğin, güvenlik, insan hakları, e-ticaret gibi) sorunlar ele alındığında, bu durum doğaları gereği çok disiplinli olan İnternet politika konularının tesirli şekilde ele alınmasını etkileyebilir. Hükümetlerden uluslararası kuruluşlara ve iş sektörüne kadar birçok aktör, siloların ötesine nasıl geçileceği ve İnternet politikası konularını geniş ve çok disiplinli bir şekilde nasıl ele alınacağı sorunu ile karşı karşıyadır.

Teknik tutarlılık ve politika tutarlılığı

İnternet yönetiřimi ile ilgili karřılařılan önemli bir zorluk da ikisi arasında açık bir ayrım yapmanın zorluğundan dolayı teknik ve siyasi yönlerle uğrařmaktır. Teknik çözümler tarafsız değıldir. Nihayetinde, her teknik çözüm/seçenek belli çıkarları destekleyerek belli gruplara güç kazandırmakta ve sosyal, siyasi ve ekonomik hayatı belli bir dereceye kadar etkilemektedir. İnternet örneğinde de, uzun bir süre boyunca hem teknik hem de siyasi yönler yalnızca bir grup tarafından idare edilmiřtir ki, o da ilk İnternet toplumdur.

İnternetin büyümesi ve yeni İnternet yönetiřimi aktörlerinin -bilhassa iş sektörü ve hükümetler-ortaya çıkması ile İnternet toplumunun teknik ve siyasi meseleleri tek bir çatı altında birleřtirmeyi sürdürmesi zorlařmıřtır. ICANN'ın kurulması da dâhil olmak üzere daha sonra yapılan reformlar teknik ve siyasi yönler arasındaki tutarlılığı yeniden sağılamaya çalıřmıřtır. Bu mesele hala sonuca ulařmamıřtır ve beklendiğı üzere gelecekteki İnternet yönetiřimi meselesine yönelik tartışmanın çekiřmeli konularından biri olarak ortaya çıkmaktadır.

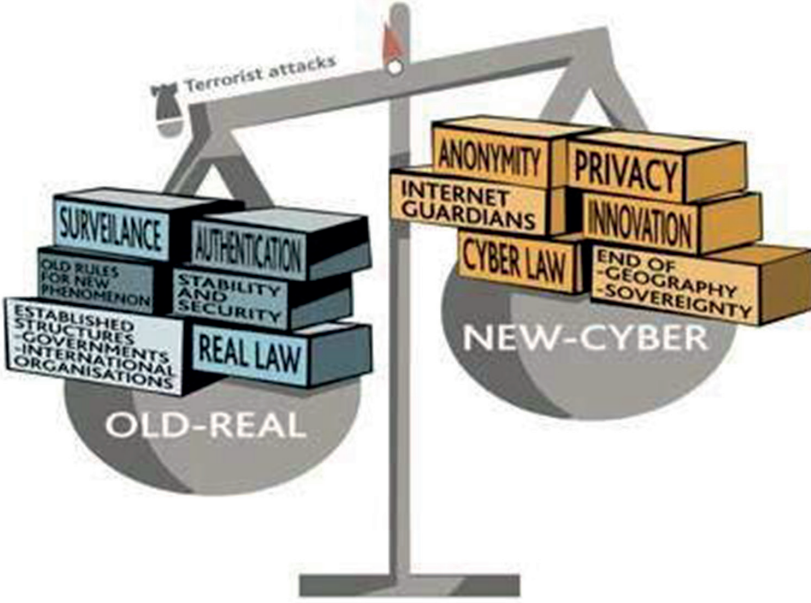
“Yeni Siber” yaklařıma karřı “eski gerçek” yaklařım

İnternet yönetiřimine yönelik her türlü meseleye getirilecek iki yaklařım bulunmaktadır (Şekil 2). “Eski gerçek” yaklařımı İnternetin yönetiřim alanına herhangi bir yenilik getirmediğini öne sürmektedir. Öncülleri olan telefon, telgraf ve radyodan herhangi bir farkı olmaksızın, yönetiřim açısından yalnızca bir diğeri yeni bir araçtır.

Örneğin yasal tartışmalarda bu yaklařım mevcut yasaların yalnızca küçük düzeltmeler ile İnternet üzerine de uygulanabileceğini öne sürmektedir. Ekonomik alanda bu yaklařım normal ticaret ile e-ticaret arasında herhangi bir farkın olmadığını ileri sürmektedir. Sonuç olarak da e-ticarete yönelik olarak özel bir yasal düzenlemeye ihtiyaç yoktur.

“Yeni siber” yaklařım ise İnternetin daha öncekilerden tamamen farklı bir iletiřim sistemi olduğunu öne sürmektedir. Siber yaklařımın ortaya attığı temel önerme, İnternetin sosyal ve siyasi gerçekliğimizi, coğrafi olarak ayrılmıř egemen devletler tarafından tanımlanan fiziksel dünyadan ayırmayı becermiř olmasıdır. Sanal alem, gerçek alemden farklıdır ve farklı bir yönetiřim biçimini gerektirir. Siber alemin yeni ve farklı bir alem olduğı görüşü NATO'nun 2016 yılındaki Varřova Zirvesinde aldığı siber alemin dünyada var olan toprak, su ve havaya ilave olarak dördüncü bir askeri alan olduğı yönündeki kararı ile de desteklenmektedir.²²

INTERNET GOVERNANCE PARADIGM Old-Real vs New-Cyber



Şekil 2. İnternet yönetişimi paradigması

Hukuk alanında sanal düşünce ekolü, yargılama, suçlar ve sözleşmelere yönelik mevcut yasaların İnternete uygulanamayacağı ve yeni yasaların oluşturulması gerektiğini ileri sürmektedir. Eski gerçeklik yaklaşımı hem düzenleyici konular hem de siyaset alanında giderek daha fazla ön plana çıkmaktadır. Ayrıca Birleşmiş Milletlerin muhtelif insan hakları sözleşmeleri offline olan insan haklarının online alanda da uygulanması prensibini kabul etmektedir.

İnternet yönetişiminde merkezi yapıya karşı adem-i merkezi yapı

Adem-i merkezîyetçi görüşe göre, İnternet yönetişimi İnternetin şu doğasını yansıtmalıdır: ağlardan oluşan bir ağ. Bu görüş İnternetin hükümetlerarası bir kuruluş gibi tek bir yönetim çatısı altına yerleştirilemeyecek kadar karmaşık bir yapıda olduğunu ve adem-i merkezî yönetişimin İnternetin hızlı gelişmesine yardım eden temel unsurlardan biri olduğunu vurgulamaktadır. Bu görüş genellikle teknik İnternet topluluğu ve gelişmiş ülkeler tarafından desteklenmektedir.

Diğer yandan merkezîyetçi yaklaşım ise İnternet yönetişimini sağlayacak uluslararası bir kuruluşun olması gerektiğini ileri sürmektedir. Bu yaklaşımın temel nedenlerinden birisi sınırlı insan kaynağı ve finansal kaynağa sahip ülkelerin, hayli adem-i merkezî ve çok kurumlu ortamda internet yönetişimi tartışmalarını takip etmede yaşadıkları zorluklar olmuştur. Bu gibi ülkeler, ICANN, W3C (Dünya Çapında AĞ Konsorsiyumu) ve IETF gibi diğer kurumların faaliyet-

lerini takip etmek bir yana dursun, ana diplomatik merkezlerde (Cenevre, New York) yapılan toplantılara dahi katılmayı zor bulmaktadır.

İnternette kamu yararının korunması

İnternetin temel güçlü yönlerinden birisi de, onun hızlı büyüme sağlamanın yanı sıra yaratıcılık ve içericiğe teşvik eden açık ve kamusal doğasıdır. İnternetin kamusal doğasının nasıl korunacağı İnternet yönetişimine yönelik tartışmanın temel meselelerinden biri olarak ortada durmaktadır. Bu sorun, temel İnternet altyapısının - kıtalar ötesi omurgalardan yerel ağlara kadar - büyük bir kısmının özel mülkiyete ait olduğu düşünüldüğünde özellikle karmaşık bir hal almaktadır. İnternetin özel sektördeki sahiplerinden interneti kamu yararını gözeterek yönetmelerinin istenip istenemeyeceği ve İnternetin hangi kısımlarının küresel kamu malı olarak düşünülebileceği ele alınması gereken zor sorulardan bazılarıdır. Örneğin, internetin temel altyapısının küresel bir kamu kaynağı olduğu görüşü Alman Araştırmacı Dennis Broeder²³ ve Malta Büyükelçisi Dr. Alex Sceberras Trigona²⁴ tarafından geliştirilmiştir. İnternetin kamusal doğasına ilişkin soru ağ tarafsızlığı tartışmalarıyla yeniden gündeme gelmiştir.

Küresel kamu malları konusunda daha fazla tartışma için 7. Bölüme bakınız.

Coğrafya ve İnternet

İnternete yönelik ilk varsayımlardan birisi ulusal sınırları aştığı ve egemenlik ilkesini yıpratmış olmuştur. İnternet iletişiminin ulusal sınırları kolaylıkla aşması ve İnternetin kendi tasarımı içerisinde gömülü kullanıcı bilinmezliği ile pek çok insana öyle gelmektedir ki, ünlü [Siber Mekanın Bağımsızlık Bildirgesi](#)'nden alıntı yapacak olursak, hükümetlerin “bizleri [yani kullanıcıları] yönetme konusunda ahlaki bir hakka sahip olmadığı” gibi “korkmamızı gerektirecek herhangi bir yaptırım yöntemine” de sahip değildir.

Ne var ki, daha karmaşık jeolokasyon yazılımları da dahil olmak üzere yakın geçmişte gerçekleşen teknolojik gelişmeler, İnternet çağında coğrafyanın bittiğine yönelik görüşe gitgide daha fazla ters düşmektedir. Aslında bu gelişmeler coğrafyanın dönüşüne işaret emektedir. İnternet kullanıcıları giderek coğrafyaya internet öncesi dönemden daha bağımlı hale gelmektedir. [Do-layısıyla, internet coğrafyaya daha bağımlı hale geldikçe internetin yönetişimi daha az özgün hale gelmektedir.](#) Örneğin İnternet kullanıcılarının ve işlemlerinin coğrafi konumunu belirleme ihtimali ile birlikte İnternete yönelik yargılama konusundaki karmaşık sorun mevcut yasalarla çözüme kavuşabilir.

Dijital teknoloji ve politika belirsizliği

İnternet teknolojisi oldukça hızlı bir şekilde gelişmektedir. Neredeyse her gün yeni hizmetler piyasaya sunulmaktadır. Bu da İnternet yönetişimi tartışmasını organize etme konusunda yeni zorlukları beraberinde getirmektedir. Örneğin, 2005 Kasım ayında mevcut İnternet yönetişimi

düzenlemesi Tunus'ta gerçekleştirilen WSIS'de müzakere edildiğinde²⁵, Twitter henüz yoktu. Bugün ise Twitter İnternet yönetişimine ilişkin gizliliğin korunması, ifade özgürlüğü gibi temel meselelerin bazılarını harekete geçirmiştir.

Spam (istenmeyen e-posta) ile mücadele teknolojinin internet yönetişimini nasıl etkilediğine ilişkin bir diğer örnektir. 2005 yılına döndüğümüzde spamın temel yönetim meselelerinden birisi olduğunu görürüz. Günümüzde oldukça karmaşık teknolojik filtreler sayesinde spam konusu İnternet yönetişimi toplantılarında nadiren gündeme gelmektedir.

Böylece, günümüzdeki politika sorunlarının bir kısmının teknolojik gelişmelerle çözülebilmektedir.

Politika dengeleyici sözleşmeler

Denge, İnternet yönetişimi ve politika tartışmalarına yönelik muhtemelen en uygun görselleştirmedir. İnternet yönetişimi ve hakkındaki pek çok hususta, çeşitli ilgi alanları yaklaşımlar arasında denge kurulması gerekmektedir. Bu dengenin kurulması büyük sıklıkla uzlaşma gerektirmektedir. Politika dengeleme alanları arasında şunlar yer almaktadır:

- **Kamu düzeninin korunmasına karşı ifade özgürlüğü:** İnsan Hakları Evrensel Bildirgesi'nin oldukça iyi bilinen iki maddesi olan Madde 19 (ifade özgürlüğü) ve Madde 29 (kamu düzeninin korunması) arasındaki tartışma İnternet konusuna da uzanmıştır. Konu genellikle İnternette içerik kontrolü ve sansür bağlamında tartışılmaktadır.

Siber güvenlik konusunda daha fazla tartışma için 3. Bölüme bakınız.

- **Özel hayatın gizliliğine karşı siber güvenlik:** Gerçek hayattaki güvenlik gibi, siber güvenlik de özel hayatın gizliliği hakkı gibi bazı insan haklarını tehlikeye atabilmektedir. Siber güvenlik ve gizlilik arasındaki denge, genel küresel siyasi duruma göre sürekli değişim göstermektedir. 11 Eylül saldırılarından sonra küresel gündemin güvenliği öne almasıyla söz konusu denge siber güvenliğe doğru kaymıştır.

Fikri mülkiyet konusunda daha fazla tartışma için 4. Bölüme bakınız.

- **Fikri mülkiyet:** Materyallerin adil kullanımına karşı yazar haklarının korunması çevrimiçi dünyaya yeni bir bakış açısı getiren bir diğer “gerçek” hukuksal ikilemdir.

Pek çok insan bu “denge ikilemlerini” yanlış ikilemler olarak eleştirmektedir. Örneğin daha fazla siber güvenliğin daha az gizlilik anlamına gelmediğine yönelik güçlü argümanlar öne sürülmektedir. Hem siber güvenliğin hem de gizliliğin geliştirilmesine yönelik yaklaşımlar da mevcuttur. Bu görüşler şiddetle savunulurken, yukarıda bahsedilen internet yönetişimi politikasının gerçeği onun muhtelif politika seçenekleri arasında tavizlerle çözümleri dengeleme arayışı tarafından şekillendiğidir.

Tekerleği yeniden icat etmeyin

İnternet yönetiřimi alanındaki her türlü giriřim iki ana gruba ayrılabilir: mevcut düzenleme ve/veya politikalarla bařlamalıdır:

- İnternet için icat edilenler (örneğin internet isimleri ve sayılarının yönetimine ilişkin ICANN düzenlemeleri, nesnelerin interneti (NesNet) alanındaki politikalar)
- İnternet ile ilgili meseleleri ele almak için önemli uyarlamalar gerektirenler mevcut politika ve düzenlemeler. Uyarlamaların düzeyi insan hakları gibi sınırlı uyarlamalardan, örneğin, siber para birimleri ve e-vergileendirme gibi daha derin konulara kadar deęiřebilir.

Mevcut kuralların kullanımı, yasal istikrarı önemli derecede artıracak ve gelecekteki dijital politika sisteminin geliřimindeki karmařıklığı azaltacaktır.

Bozulmamıřsa tamir etme

İnternet yönetiřimi, İnternetin mevcut iřlevsellięini ve saęlamlięını devam ettirmeli, ancak artan iřlevsellik ve daha fazla meřruiyete yönelik deęiřiklikleri de kabul edebilecek kadar esnek kalmalıdır. Genel kanaat İnternetin istikrarı ve iřlevsellięinin İnternet yönetiřimine kılavuzluk eden ilkelerden birisi olması gerektięidir.

İnternetin istikrarı, teknik altyapıda doęru řekilde test edilmiř deęiřikliklerin zamanla uygulanmasını gerektiren “çalıřan kod” (running code) adlı ilk İnternet yaklařımı vasıtasıyla sürdürülmüřtür. Ancak bazı aktörler “çalıřıyorsa kurcalama” sloganının kullanımının mevcut İnternet yönetiřimindeki teknik altyapı ile ilgisi olmayan deęiřiklikler de dahil olmak üzere her türlü deęiřiklięe karřı baęıřıklık saęlayacaęından endiře duymaktadır. Bir çözüm de bu ilkenin Belirlenen İnternet yönetiřimi ile alakalı kararların deęerlendirilmesine yönelik bir kriter olarak bu ilkenin belirli internet yönetiřimi ile ilgili kararların deęerlendirilmesi için bir kriter olarak kullanılmasıdır (örneğin, karar verme mekanizmalarında yeni protokol ve deęiřikliklerin getirilmesi gibi).

Bütünsel bir yaklařımın teřviki ve önceliklendirme

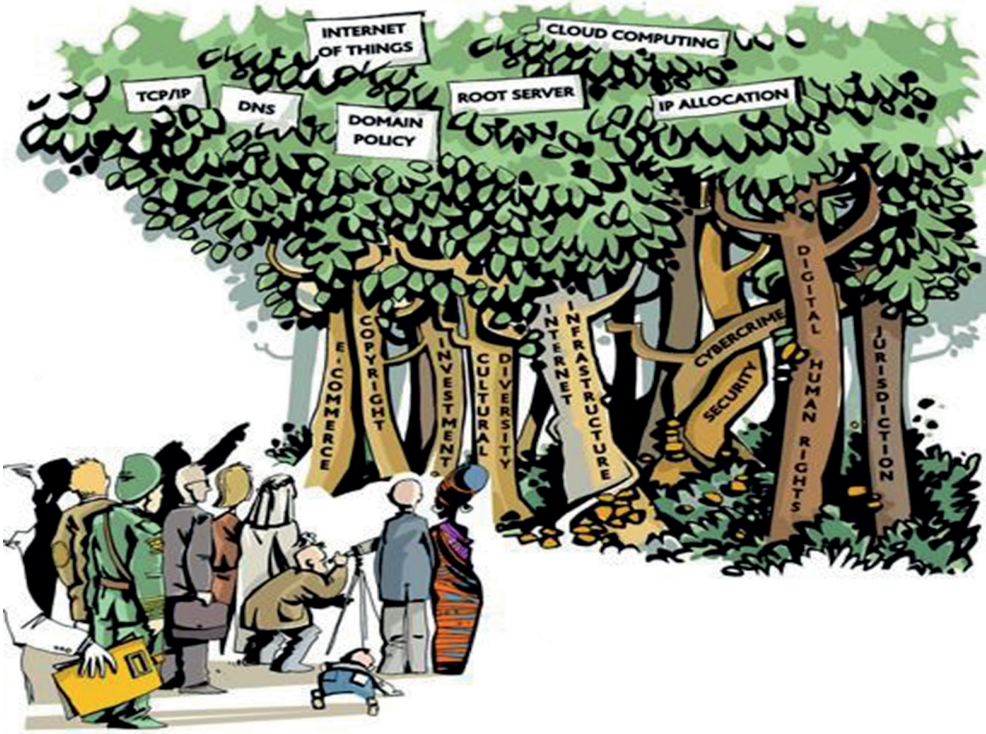
Bütünsel bir yaklařım İnternet geliřiminin yalnızca teknik deęil aynı zamanda yasal, sosyal, ekonomik ve geliřimsel, güvenlik ve insan haklarıyla ilgili boyutları da ele almayı kolaylařtırmalıdır. Bu yaklařım aynı zamanda telekomünikasyon hizmetleri alanına yönelen internet řirketleri (örneğin, deniz altına kablolar döřeyen Google, Facebook gibi) ve dijital içerikli servis saęlayan telekomünikasyon řirketleri ile birlikte dijital teknolojiye giderek artan birleřmeleri de göz önüne almalıdır.

İnternet yönetiřimi müzakerelerine yönelik olarak bütünsel bir yaklařımı sürdürürken, paydařlar internet yönetiřimi ormanını görüř alanlarından çıkarmaksızın kendi ilgi alanlarına göre öncelik vereceęi meseleleri belirlemelidirler (řekil 3).

Ne geliřmekte olan ne de geliřmiř ülkeler homojen gruplar deęildir. Geliřmekte olan ülkeler

arasında, öncelikler, gelişim düzeyi ve bilgi teknolojilerine hazır oluşluk (IT readiness) açısından muazzam farklılıklar bulunmaktadır (örneğin, Hindistan, Çin ve Brezilya gibi bilgi ve iletişim teknolojileri açısından gelişmiş ülkeler ile sahra altı Afrika gibi en az gelişmiş ülkeler bulunmaktadır).

İnternet yönetişimi gündemine yönelik bütünsel bir yaklaşım ve önceliklendirme hem gelişmiş hem de gelişmekte olan ülkelere gelen paydaşların belirli bir takım meselelere odaklanmasına yardımcı olmalıdır. Bu da daha esaslı ve muhtelemelen daha az politikleşmiş müzakerelere yol vermelidir. Paydaşlar geleneksel olarak hayli politikleşmiş çizgilerden ziyade meseleler etrafından gruplaşabilirler (Örneğin, gelişmiş-gelişmekte olan ülkeler, hükümetler-sivil toplum gibi).



Şekil 3. İnternet yönetişimi

Teknolojik tarafsızlık

Teknolojik tarafsızlık ilkesine göre, politika belirli teknolojiler veya teknik araçlar için tasarlanmamalıdır. Örneğin, özel hayatın gizliliğinin korunmasına yönelik düzenlemeler gizliliğin nasıl korunacağını değil (örneğin, veritabanına erişim, kriptokoruma gibi) neyin korunması gerektiğini (örneğin, kişisel veriler, sağlık kayıtları gibi) belirtmelidir.

Teknolojik tarafsızlık pek çok yönetim avantajını da beraberinde getirmektedir. Bu ilke gelecekteki teknolojik gelişmelerden bağımsız olarak yönetişimin sürekli geçerliliğini ve belli başlı

teknolojilerin muhtemel birleşmesini (telekomünikasyon, medya, İnternet vs.) sağlamaktadır. Teknolojik tarafsızlık ağ tarafsızlığından farklıdır: ilki belirli bir politikanın düzenlediği teknolojiden bağımsız olduğunu gösterir, diğeri ise temel olarak İnternet trafiğinin tarafsızlığı üzerine odaklanmaktadır.

Zımnî bir politika olarak teknolojik çözümler

Serbest iletişim gibi belirli sosyal değerlerin, İnternetin teknolojik olarak tasarlanması yoluyla kolaylaştırıldığı İnternet toplumu içerisinde yaygın olarak benimsenen bir görüştür. Örneğin ağın araçları ortaya koymaksızın yalnızca iki uç noktası arasında veri transferi yapması gerektiğini öne süren ağ tarafsızlığı ilkesi genellikle İnternet üzerinde özgürce iletişim kurma garantisi olarak kabul görmektedir. Bu görüş bizi, teknolojik çözümlerin sosyal değerleri koruma ve desteklemede yeterli olduğu gibi yanlış bir sonuca götürmektedir. İnternet alanında yaşanan bilgi akışının engellenmesi için güvenlik duvarı kullanımı gibi en son gelişmeler teknolojinin pek çok, hatta görünüme göre birbiriyle çelişen şekillerde kullanılabileceğini kanıtlamaktadır. Mümkün oldukça, serbest iletişim gibi ilkeler teknik düzeyde üstü örtük biçimde değil, politika düzeyinde açıkça ifade edilmelidir. Teknolojik çözümler politika ilkelerini güçlendirmeli ancak onları destekleyecek tek yol olma niteliğini taşımamalıdır.

Toplumu algoritmalar yoluyla çalıştırma

Teknoloji ve politika arasındaki ilişkinin temel bir özelliği, İnternete gittikçe artan bağımlılıktan ötürü modern toplumun bir gün kendisini yasal kurallar yerine yazılım kodları ile düzenleniyor şekilde bulacağını gözlemleyen Lawrence Lessig tarafından tanımlanmıştır. En nihayetinde parlamento ve hükümetin bir takım yasama işlevleri, bilgisayar şirketleri ve yazılım geliştiriciler tarafından fiilen ele geçirilebilir. Yazılım ve teknik çözümlerin bir araya gelerek gitgide İnternete bağlı bir hal alan toplumlarda, hayatı etkileyebilir. Yapay zekaya (AI) dayalı bir dizi yeni teknolojinin insanların aldıkları kararların alınmasını makinalara transfer etmesi beklenebilir. Günümüzde en canlı tartışmalardan birisi sürücüsüz arabalarla ilgili gelecekteki düzenlemelerdir. Modern toplum günlük faaliyetlerde insanın yerini alan makinalar ile toplumumuzun siyasi ve yasal örgütlenmesini ilgilendiren kararları alan makinalar arasındaki sınırı tanımlamak ve bununla uğraşmak zorunda kalacaktır.

Analojiler

Analoji genellikle yanıltıcı olsa da, sahip olduğumuz en az yanıltıcı şeydir.

Samuel Butler, İngiliz Şair (1835–1902)

Analoji bizim yeni gelişmeleri bilinenler açısından anlamamıza yardımcı olur. Geçmişteki ve şu anki örnekler arasında paralellikler çizmek, taşıdığı risklere rağmen hukuk ve siyaset alanındaki

temel bilişsel süreçlerden birisidir. İnternete ilişkin yasal durumların pek çoğu, özellikle Anglo-Sakson kökenli hukuk sisteminde analogiler vasıtasıyla çözülmektedir. Analogilerin İnternet yönetiminde kullanımı bazı önemli sınırlandırmalara sahiptir.

Öncelikle, “İnternet” (telefona benzetilebilen) e-posta, (televizyon gibi yayın hizmetlerine benzetilebilen) web hizmetleri, (kütüphanelere benzetilebilen) veri tabanları ve (kafeler veya pazarlara benzetilebilen) sosyal medya gibi çeşitli hizmetleri kapsayan geniş bir terimdir. İnternetin belirli herhangi bir yönü ile kurulacak bir benzerlik İnternete ilişkin anlayışı sınırlı açılara indirgeyebilir.

İkinci olarak, farklı telekomünikasyon ve medya hizmetlerinin gittikçe artan şekilde birleştirilmesi ile birlikte çeşitli hizmetler arasındaki geleneksel farklılıklar belirsizleşmektedir. Örneğin İnternet Üzerinden Sesli İletişimin (VoIP) tanıtılması ile İnternet ve telefon hizmeti arasında kesin bir ayırım yapmak güç bir hal almıştır. Sınırlayıcı bu unsurlara rağmen, analogileri hala güçlüdür ve hala yasal meseleleri çözmede ve İnternet yönetimi rejimini geliştirmede temel bilişsel araç olmaya devam etmektedir.

Üçüncü olarak, analogiler İnternet’in ilk günlerinde, yeni bir araç ve fenomen olduğunda çok önemliydi. Örneğin, bu kitabın ilk baskısında (2004), analogiler interneti açıklamak için çok önemliydi. İnternetin büyümesiyle analogiler daha az alakalı hale geldi. Genç nesiller artık internet ile büyüyor. Bu araştırmadaki bazı analogiler (video kaset kaydediciler - VCR’ler gibi) onlara arkaik gelebilir. Bununla birlikte, analogiler, İnternet yönetişimini şekillendiren birçok mahkeme kararı ve politikalar temeli olarak önemini korumaktadır. Dolayısıyla, analogilerle ilgili aşağıdaki özetinin hem İnternet yönetiminde analogilerin kullanımının tarihsel bir kaydı hem de dijital politikadaki güncel gelişmelerin köklerini yorumlama aracı olarak sunulması amaçlanmaktadır.

İnternet – telefon

Benzerlikler: İnternetin ilk günlerinde, bu analogi telefonun çevirmeli erişim ile İnternete bağlanmak üzere kullanılmasından etkilenmiştir. Bunun yanı sıra, her ikisi de doğrudan ve kişisel birer iletişim yolu olan telefon ve İnternet arasında işlevsel bir analogi de yer almaktadır (e-posta ve sohbet).

Farklılıklar: Telefon devre hatlarını kullanırken internet, hatlar yerine paketleri kullanmaktadır. Telefon hizmetinin aksine, İnternet hizmetlerinin garantisini vermez, yalnızca “en iyi çaba” garantisini vermektedir. Analogi İnternetin yalnızca bir yönünün altını çizmektedir: e-posta veya sohbet yoluyla iletişim. Dünya Çapında Ağ (World Wide Web), interaktif hizmetler vs. gibi belli başlı diğer İnternet uygulamaları telefon ile aynı özellikleri paylaşmamaktadır.

Kullanıcılar: Bu analogi İnternet içeriğinin düzenlenmesine karşı çıkanlar tarafından kullanılmaktadır. Eğer İnternet telefonla benzer ise, İnternet iletişiminin içeriği - örneğin yayıncılığın aksine - yasal olarak kontrol edilemez. Bu analogi aynı zamanda İnternetin tıpkı diğer iletişim sistemleri (örneğin, telefon hizmeti, posta) gibi ITU benzeri uluslararası kuruluşların koordine edici rolüne sahip ulusal otoriteler tarafından idare edilmesi gerektiğini savunanlar tarafından

kullanılmaktadır. Bu analogiye göre İnternet DNS’i telefon hizmetindeki numaralandırma sistemi gibi organize edilmeli ve idare edilmelidir.²⁶

Karmaşık analogide yeni bir dönüm noktası da İnternet protokollerini kullanırken telefon işlevi gören VoIP (örneğin, Skype) ile ortaya çıkmıştır. Bu ikilem Dubai’de gerçekleştirilen Dünya Uluslararası Telekomünikasyon Konferansı’nın (WCIT) hazırlık aşamasında bir politika anlaşmazlığı tetiklemiştir. VoIP’in İnternet hizmeti olduğu konusundaki mevcut görüşe, onun bir telekomünikasyon hizmeti olduğunu ve telefon hizmeti gibi ITU tarafından küresel düzeyde düzenlenmesi gerektiğini savunanlar tarafından karşı çıkmıştır.

İnternet – posta/ileti

Benzerlikler: Bu analogi ortak bir işleve dayandırılmıştır, yani mesajların iletilmesi. İsmi kendisi yani e-posta bu benzerliği yansıtmaktadır.

Farklılıklar: Bu analogi yalnızca tek bir İnternet hizmetini kapsamaktadır: e-posta. Bunun yanı sıra, posta hizmeti gönderici ve alıcı arasında, aktif aracılık işlevinin ISP veya Yahoo! veya Hotmail gibi bir e-posta hizmet sağlayıcısı tarafından yürütüldüğü e-posta hizmetinden çok daha karmaşık bir aracı yapıya sahiptir.

Kullanan: Dünya Posta Konvansiyonu e-postayı: “mesajların elektronik olarak iletilmesini de kapsayan bir posta hizmeti” olarak tanımlamaktadır. Bu analogi resmi belgelerin iletilmesine ilişkin sonuçlar doğurabilmektedir. Örneğin bir mahkeme kararının e-posta yoluyla teslim alınması resmi bir teslim olarak düşünülebilir.

Irak’ta ölen Amerikan askerlerinin aileleri tıpkı mektup ve günlüklerde olduğu gibi e-posta ve blogları da miras yoluyla devralmaları gerektiğini savunarak bu benzerliği aynı zamanda sevdiklerinin kişisel e-postalarına veya bloglarına erişim sağlayabilmek amacıyla, posta (mektuplar) ve e-posta arasında da benzerlik kurmaya çalışmışlardır. İnternet servis sağlayıcılar (ISPs) oldukça duygusal bu tarz sorunlarla baş etmekte zorlanmıştır. Mektup ile e-posta arasındaki benzerliği kabul etmek yerine, pek çok ISP, kullanıcıları ile imzalamış oldukları gizlilik sözleşmesine dayanarak erişimi engellemiştir.

Posta sistemi ve ICANN

ICANN’in önceki yöneticisi Paul Twomy posta sistemi ve ICANN’in işlevi konusunda aşağıdaki analogiyi kullanmıştır: “Eğer interneti bir postane veya bir posta sistemi gibi düşünürseniz, alan isimleri ve IP adresleri özellikle zarfın üzerindeki adresi güvenceye alma işlevi görmektedir. Bunlar zarfın içine ne koyduğunuz, zarfı kimin gönderdiği, zarfı kimin okumasına izin verildiği, zarfın ne kadar sürede gönderileceği ve zarfın fiyatı ile ilgili konular değildir. Bu konuların hiç biri ICANN’in işlevleri açısından önemli değildir. İşlev adresin doğru olduğunun güvenceye alınmasına odaklanmaktadır.”

İnternet – televizyon

Benzerlikler: İlk analogi bilgisayarlar ile televizyon ekranları arasındaki fiziksel benzerlik ile alakalı olmuştur. Daha karmaşık bir analogi ise her iki medyanın, yani web ve TV’nin yayın yapma amacıyla kullanılmasıdır.

Farklılıklar: İnternet televizyondan daha geniş kapsamlı bir araçtır. Bilgisayar ekranı ile TV ekranı arasındaki benzerlik bir yana dursun, her ikisi arasında belli başlı yapısal farklılıklar bulunmaktadır. Televizyon bir çok izleyiciye bir noktadan yayın yapmak için kullanılan birden-çoğa şeklinde bir araç iken, İnternet farklı tipte pek çok iletişimi kolaylaştırmaktadır (birden-bire, birden-çoğa, çoktan-çoğa gibi).

Kullanan: Bu analogi İnternet içeriği üzerine daha sıkı bir kontrol getirilmesini isteyenler tarafından kullanılmaktadır. Savundukları görüşe göre, televizyona benzer şekilde bir kitle iletişim aracı gücüne sahip olduğundan, İnternetin sıkı bir şekilde denetlenmesi gerekmektedir. ABD hükümeti bu analogiyi cıgır açıcı Amerikan Sivil Özgürlükler Birliği’nin Reno’ya karşı açtığı davada²⁷ kullanmaya çalışmıştır. Bu dava Kongre tarafından kabul edilen ve çocukların İnternet aracılığıyla pornografik içeriğe maruz kalmasını önlemek amacıyla sıkı bir içerik kontrolünü gerektiren İletişim Ahlakı Yasası ile hatırlanmaktadır. Mahkeme televizyon benzerliğini tanımayı reddetmiştir.

İnternet – kütüphane

Benzerlikler: İnternet bazen bilgilerin depolandığı büyük bir alan olarak görülmekte ve “kütüphane” terimi genellikle bunu tarif etmek için kullanılmaktadır: örneğin, “büyük dijital kütüphane”, “siber kütüphane”, “21. Yüzyılın İskenderiye Kütüphanesi” gibi.

Farklılıklar: Bilgi ve verilerin depolanması İnternetin yalnızca bir yönü olup, kütüphaneler ile İnternet arasında muazzam farklılıklar bulunmaktadır:

- Geleneksel kütüphaneler belirli bir mekanda (şehir, ülke vb.) yaşayan bireylere hizmet etmeyi amaçlarken, İnternet küreseldir.
- Kitaplar, makaleler ve dergiler kaliteyi sağlamak için bir takım prosedürler kullanılarak basılırlar (editörler). İnternette daima editörler bulunmaz.
- Kütüphaneler kullanıcıların koleksiyonlarındaki kitapların yerini bulmalarına izin verecek şekilde belirli sınıflandırma şemalarına göre düzenlenmiştir. İnternet üzerindeki bilgiler için bu tarz herhangi bir sınıflandırma söz konusu değildir.
- Anahtar kelime tariflerinin yanı sıra, kütüphane içeriği (kitap ve makale metinleri) kullanıcı belirli bir kitap veya dergiyi ödünç alana kadar erişilebilir değildir. İnternet içeriğine ise arama motorları vasıtasıyla hemen ulaşılabilir.

Kullanan: Bu analogi belirli konular üzerinde kapsamlı bir bilgi ve birikim sistemi oluşturmayı amaçlayan çeşitli projeler tarafından kullanılmaktadır (portallar, veritabanları vs.). Son zamanlarda kütüphane analogisi, tüm basılı kitapların dijitalleştirilmesi amacını güden Google kitap projesi bağlamında kullanılmaktadır.

İnternet – VCR, fotokopi makinası

Benzerlikler: Bu analogi içeriğin (örneğin, metinler ve kitaplar gibi) yeniden üretimi ve yayılması üzerine odaklanmıştır. Bilgisayarlar “kopyala ve yapıştır” süreci ile yeniden üretimi kolaylaştırmıştır. Bu da karşılığında İnternet yoluyla bilginin yayılmasını çok daha kolay bir hale getirmiştir.

Farklılıklar: İnternet üzerinden kopyalama eyleminin kendisi VCR veya fotokopi makinesi ile kopyalamaktan çok daha kolay olsa da, bilgisayar içeriğin kopyalanmasından çok daha geniş çaplı bir işleve sahiptir.

Kullanan: Bu analogi, telif hakkı ihlalinde (telif hakkı korumasını ihlal ederek yazılım geliştirme vs.) payı olan kurumları cezalandıran ABD’nin [Dijital Milenyum Telif Hakkı Yasası](#) (DMCA) bağlamında kullanılmaktadır. Böyle durumlarda karşıt sav olarak VCR ve fotokopi makinesi üreticileri gibi yazılım geliştiricilerin ürünlerinin yasadışı olarak kullanılıp kullanılmayacağını tahmin edemediği öne sürülmüştür.

Bu analogi, dosyaların denkler arası paylaşımında (P2P) Grokster ve StreamCast gibi Napster tarzı yazılım geliştiricilerinin aleyhine durumlarda kullanılmaktadır.

İnternet – karayolu

Benzerlikler: Gerçek dünyada karayolu ulaşım için neyi ifade ediyorsa, İnternet de sanal âlemde iletişim aynı şeyi ifade etmektedir.

Farklılıklar: İnternetin veri taşımacılığı dışında, İnternet ile karayolları arasından başka herhangi bir benzerlik yoktur. İnternet soyut içerikleri (veriler) taşıırken, karayolları mal ve insanların taşınmasını sağlamaktadır.

Kullanan: Karayolu analogisi 1990’lı yılların ortalarında, iddialara göre Al Gore ‘bilgi otobanı’ terimini icat ettikten sonra yoğun bir şekilde kullanılmıştır. “Karayolu terimi” aynı zamanda 1997 Haziran ayında daha katı bir İnternet içeriği denetim kanununun getirilmesini haklı göstermek için Alman hükümeti tarafından kullanılmıştır:

Bu kanun sansür ile hiçbir ilgisi olmayan, ancak bir hizmet sağlayıcısının neleri yapıp neleri yapamayacağı konusundaki şartları açıkça belirleyen liberal bir kanundur. İnternet tıpkı karayolları gibi bilgiyi taşıma ve dağıtma aracıdır, her iki tür trafik için de bir takım esasların var olması gerekmektedir.²⁸

Karayolları ve İnternet

Önceki ITU Genel Sekreteri Hamadoun Touré karayolları ile İnternet arasında, karayollarını telekomünikasyon, İnternet trafiğini ise kamyonlar ve arabalar ile ilişkilendirerek bir analogi yapmıştır: “İnternet ve telekomünikasyonu kamyonlar veya arabalar veya karayolları ile kıyaslayarak basit bir örnek veriyordum. Örnek vermemin sebebi üzerlerinde giden tüm kamyon veya arabalara sahip olacağınız karayollarına sahip olmanız değil, taşıdıkları mallara sahip olmanız hiç değil veya tam tersi. Bu çok basit bir analogi. Ancak trafiğinizi akıcı kılmak yollarınızı yaparken kamyonların ağırlığı, yüksekliği ve hızlarını bilmeniz lazım ki ona göre köprüler inşa edebilirsiniz. Aksi takdirde sistem akmayacaktır. Bana göre İnternet ile telekomünikasyon dünyası arasındaki ilişkide böyledir. Beraber çalışmaya mahkûmdurlar.”²⁹

İnternet – açık denizler

Benzerlikler: Bu analogi ilk olarak açık deniz suları gibi İnternetin de her türlü ulusal yargı yetkisinin ötesinde görünmesinden dolayı yapılmıştır.

Farklılıklar: İnternet ve açık deniz suları arasında birbirine uyan hiç bir yön yoktur. İlk olarak, internet verileri daima ulusal yargının alanı içerisinde kalmaktadır. Deniz altına döşeli telekomünikasyon kabloları Pasifik ve Atlantik okyanuslarında açık deniz yatakları boyunca uzanmaktadır, fakat bu kablolar ağırlıklı olarak yasal olarak kurulu bulundukları ulusal yargıya tabi özel sektörün elindedir. Eğer Microsoft veri merkezlerini açık denizlere yerleştirseydi (ki, bu şirketin düşünmekte olduğu bir şeydir), yine de Microsoft ABD’de kurulu bulunduğu için ABD yargısına tabi olacaktı. Açık denizlerdeki her aygıt, kablolar veya açık denizde işleyen gemiler bir şekilde bir ulusal yargıya bağlı olmak zorundadır.

Kullanan: Açık deniz analogisi bir çok görüşü desteklemek amacıyla kullanılmaktadır. Bazen internetin uluslararası düzenlemelere ihtiyacı olduğunu haklılaştırmak için kullanılmaktadır. Somut olarak konuşursak, bu analogi eski Roma hukukundaki res communis omnium (herkes insanlığın ortak mirasının bir parçası olan ve tüm uluslar tarafından düzenlenmesi ve hasat edilmesi gereken bir alan) kavramının, tıpkı açık denizlere yönelik düzenlemelerde olduğu gibi İnternet üzerinde de kullanımını öne sürmektedir. Bazı durumlarda ise, açık deniz analogisi internetin açık açık denizlere ilave olarak tıpkı Güney kutbu ve dış uzay gibi herhangi tek bir ülkenin ulusal yargısının dışında bir alan olduğu görüşü ile internetin ulusal olarak düzenlenmesine karşı bir görüşle kullanılmaktadır.

İnternet yönetişimi meselelerinin sınıflandırılması

İnternet yönetişimi, ilk olarak kavramsal bir haritalandırma ve sınıflandırma yapılmasını gerektiren karmaşık yeni bir alandır. Karmaşıklığı çok disiplinli oluşu, teknoloji, sosyo-ekonomi, kalınma, hukuk ve siyaset de dahil olmak üzere çeşitli alanları kapsamasından ileri gelmektedir.

Pratikte bir sınıflandırma yapma ihtiyacı WSIS süreci esnasında açıkça belirtilmiştir. İlk aşamada, Cenevre zirvesine zemin hazırlama sürecinde (2003) ulus devletler de dâhil olmak üzere

pek çok oyuncu İnternet yönetişiminin karmaşıklığını kavrama konusunda güçlük yaşamıştır. Çeşitli akademik girdiler ve WGIG raporundan verilerle hazırlanan kavramsal bir harita WSIS süreci bağlamında gerçekleştirilen müzakerelerin daha etkin bir şekilde sürdürülmesine katkıda bulunmuştur. WGIG raporu (2004) dört temel alanı tanımlamıştır:

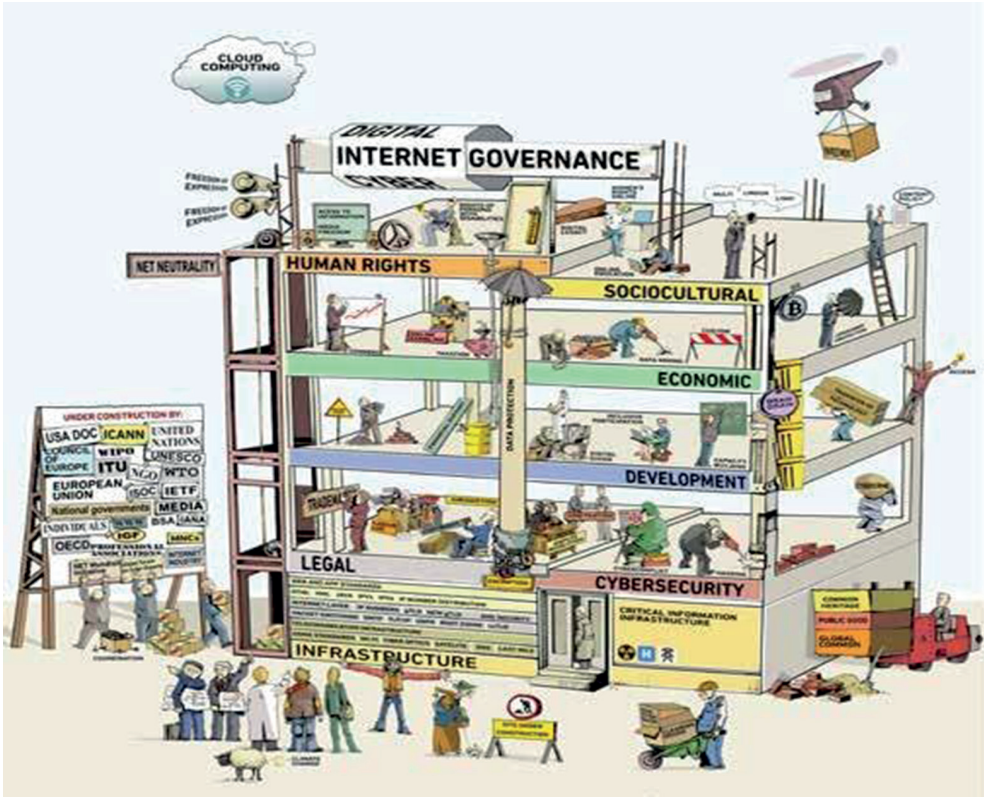
- Kritik İnternet kaynaklarının (CIR) altyapısı ve yönetimi ile ilgili meseleler,
- Spam, ağ güvenliği ve siber suçlar da dahil olmak üzere internet kullanımına ilişkin meseleler,
- İnternet ile ilişkili ancak İnternette çok daha geniş alanda etki eden ve mevcut kuruluşların sorumlu olduğu fikri mülkiyet hakları (IPR) veya uluslararası ticaret gibi meseleler,
- İnternet yönetişiminin gelişimsel yönleri ile alakalı meseleler, özellikle gelişmekte olan ülkelerde kapasite geliştirme.

Atina'da düzenlenen ilk IGF'nin (2006) gündemi aşağıdaki tematik alanlar etrafından geliştirilmiştir: erişim, güvenlik, açıklık, çeşitlilik. Rio de Janerio'da gerçekleştirilen ikinci IGF'de (2007), beşinci tematik alan gündeme eklenmiştir: Kritik İnternet kaynaklarının yönetimi. Bu beş tematik alan sonraki IGF toplantılarının gündemini etkilemiştir.

Sınıflandırma değişse de, İnternet yönetişimi, değişen belirli meselelere yönelik az ya da çok aynı 40-50 belirli konuyu ele almaktadır. Örneğin spam konusu 2004'te gerçekleştirilen WGIG'de önemli ölçüde göze çarparken, IGF toplantılarında Güvenlik tematik alanında daha az önemli konulardan birisi haline gelerek siyaset ile olan ilişkisi azalma göstermiştir.

Diplo'nun İnternet yönetişimi sınıflandırması belli başlı 40-50 konuyu aşağıdaki yedi boyutta gruplandırmıştır³⁰:

- Altyapı
- Güvenlik
- Hukuk
- Ekonomi
- Kalkınma
- Sosyokültür
- İnsan hakları



Şekil 4. Yapımı sürmekte olan internet yönetişimi

Bu sınıflandırma (Şekil 4)) hem yukarıda bahsedilen (WGIG, IGF) politika yaklaşımlarını hem de bu alandaki akademik araştırmaları yansıtmaktadır. Sınıflandırma 1997 yılında geliştirilmiş ve öğrencilerden (2015 yılı itibarıyla 3000 mezun öğrenci) alınan geri bildirimlere, araştırma sonuçlarına ve politika sürecinden elde edilen içgörülere (kavrayışlar) ve veri madenciliğine dayalı olarak düzenli olarak uyarlanmıştır. [Uluslararası internete ilişkin kamu politikası konularının haritalandırılması](#) CSTD sekreteryası tarafından 2014 Kasımında Komisyonun Dönemlerarası Panelinde hazırlanmıştır.³¹

İnternet yönetişimini isimlendirmek, tanımlamak ve çerçevesini çizmek

Önceki sayfalarda, İnternet yönetimi kavramını tanımlamanın ve çerçevelemenin alternatif yollarını tartışmıştık. Kavram (Şekil 4'te) canlı biçimde gösterildiği üzere tartışmaya açık kalmaya ve farklı yorumlarla değerlendirilmeye devam edecektir. Binanın en tepesinde “İnternet yönetişimi” adında bir afiş bulunmaktadır; Afiş, İnternet yönetişimini siber yönetim veya dijital yönetim ile kolayca değiştirmemizi sağlayan dönen bir bölüme sahiptir. Kamu politikası tartışmalarında, İnternet politikası, dijital politika ve siber diplomasi gibi diğer terimler de kullanılmaktadır.

Tartışma, İnternet yönetiminin kapsamını, yani kendi meseleleri içinde kalan sorunları da eklediğimizde daha da karmaşık hale gelmektedir. Örneğin, bazıları siber güvenliğin İnternet yönetiminin bir parçası olduğunu savunmaktadır. Diğer bazıları da siber güvenliğin ayrı bir alan olduğunu savunmaktadır. Bazıları İnternet yönetişiminin yalnızca ICANN ile ilgili konular (etki alanı adlarının, IP adreslerinin vb.) olduğunu söylemektedir. Diğer bazıları, İnternet yönetişimi kapsamını, İnternet ile ilgili geniş bir kamu politikası konuları setine dayandırmaktadır.

Bu tartışma sadece teorikle alakalı değildir. Ayrıca, İnternet politikası konularının nerede, nasıl ve kim tarafından tartışıldığı ve ele alındığı ile ilgili pratik yönleri de etkilemektedir. Terimler ve tanımlar konusundaki bu tartışmanın basit bir çözümü yoktur. Farklılıklar devam edecektir ve nihayetinde hepimizin hemfikir olacağı “doğru” bir terim ve tanımın ortaya çıkma ihtimali yok gibidir.

Bu kitapta, İnternet yönetişimi, 7 sepette gruplanmış 40'tan fazla İnternet kamu politikası meselesini kapsayan bir şemsiye kavram olarak kullanılmıştır. Bu yaklaşım, WGIG'in İnternet yönetişimi tanımından ve terimin WSIS süreçlerinde, yayınlarda ve akademik araştırmalarda kullanılma şekline ilham almıştır. Farklı terimlerin ve tanımların kullanımı, diğer politika ve araştırma gerekçelerinden ilham almıştır.

“Doğru” terim veya tanım tartışmasının özellikle etkili veya faydalı olması muhtemel olmasa da, her bir terimin tam olarak kapsamının net bir şekilde anlaşılması bakımından çok önemlidir. Örneğin, İnternet yönetişimi, dijital politika veya siber yönetim kavramları altından hangi konular tartışılmaktadır? İnternet kamu politikası meselelerinden yalnızca birkaçını belirlemek adına bu kavramlar siber güvenlik, e-ticaret veya çevrimiçi gizlilik konularını kapsıyor mu? Her bir terimin kapsamını anlamak, politika süreçlerinde karışıklığı azaltmaya ve netliği arttırmaya yönelik ilk adım olacaktır.

Sonuç olarak, dijital araçların modern toplumda kusursuz bir şekilde bütünleşmesiyle, terminoloji konusundaki tartışma daha az öneme sahip olacaktır. E-ticaret, ticaretin vazgeçilmez bir parçası olarak yerini alacaktır. Siber güvenlik, güvenlik öncelikleriyle uyum sağlamaya ve onları desteklemeye devam edecektir. Dijital gelişme günlük hayatımızın daha fazla içsel bir parçası haline geldikçe, İnternet yönetişiminin toplumun temelindeki yönetime uyum sağlama olasılığı da artacaktır.

Son notlar

- 1 BM Genel Kurulu Kararı 56/183 (21 Aralık 2001) Bilgi Toplumu Dünya Zirvesi'nin (WSIS) iki aşamada düzenlenmesini Ekim. İlk aşama 10- 12 Aralık 2003 tarihleri arasında Cenevre'de, ikinci aşama ise 16- 18 Aralık 2005 tarihleri arasında Tunus'ta gerçekleştirilmiştir. İlk aşamanın amacı siyasi niyete yönelik açık bir bildirimin geliştirilmesi ve teşvik edilmesi ve herkes için söz konusu farklı çıkarları yansıtan bir Bilgi Toplumu'nun temellerinin atılması için somut adımlar atılması olmuştur. 174 ülkeden 19000'i aşkın katılımlı zirveye ve ilgili aktivitelere katılmıştır. Kaynak: <http://www.itu.int/wsis/basic/about.html> [Erişim 28 Eylül 2016].
- 2 WGIG tanımı rejim teorisinde sıkça kullanılan tanımların yapısını izlemektedir. Rejim teorisinin kurucusu Stephen D. Krasner şunu belirtmektedir: Rejimler, aktörlerin beklentilerinin mevcut bir uluslararası ilişkiler alanında birleştiği açıkça belirtilen veya belirtilmeyen ilkeler, normlar ve karar verme prosedürleri olarak tanımlanabilir. İlkeler doğruluk, sebep ve gerçek fikirlerdir. Normlar haklar ve yükümlülükler açısından tanımlanan davranış standartlarıdır. Kurallar eyleme yönelik belli talimat veya yasaklamalardır. Karar verme prosedürleri kolektif bir tercihin yapılması ve uygulanması için mevcut olan uygulamalardır. Krasner S (1983) Introduction, International Regimes. Krasner SD (ed.), Cornell University Press: Ithaca, NY, ABD.
- 3 Shannon V (2006) What's in an 'i'? International Herald Tribune, 3 Aralık 2006. <http://www.nytimes.com/2006/12/03/technology/03iht-britu.3755510.html> [Erişim 28 Eylül 2016].
- 4 Barlow JP (1996) A declaration of the independence of cyberspace. <https://www.eff.org/cyberspace-independence> [Erişim 28 Eylül 2016].
- 5 WSIS Zirvesinin hazırlığında "İnternet" kelimesinin evrimi için: DiploFoundation (2003) The Emerging Language of ICT Diplomacy – Key Words. <https://www.diplomacy.edu/IGFlanguage/2004research> [Erişim 3 Ağustos 2014].
- 6 Working Group on Internet Governance (2005) Report. <http://www.wgig.org/docs/WGIGREPORT.pdf> [Erişim 10 Ekim 2016].
- 7 World Summit on the Information Society (2005) Tunis Agenda for the Information Society. <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> [Erişim 10 Ekim 2016].
- 8 2010 Haziran ayında, ICANN yetişkin içeriği için XXX üst düzey alan adının kullanımını onaylamıştır.
- 9 Ağ tarafsızlığı ilgili olarak linkteki açıklayıcı videoyu izleyin <https://www.youtube.com/watch?v=R-uMbZFfjVU> [Erişim 3 Ekim 2016].
- 10 Clinton H (2010) Remarks on Internet freedom. <http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm> [Erişim 3 Ekim 2016].
- 11 13-16 Temmuz 2015'te gerçekleştirilen Ababa Action Agenda'nın Üçüncü Uluslararası Kalkınma Finansmanı Konferansında gündeme getirilen 123. Paragrafı. http://www.un.org/esa/ffd/wp-content/uploads/2015/08/AAAA_Outcome.pdf [Erişim 10 Ekim 2016].
- 12 World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 3 Ekim 2016].
- 13 Drake W et al. (2016) Internet Fragmentation: An Overview. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [Erişim 3 Ekim 2016].
- 14 Global Commission on Internet Governance (2016) One Internet. <https://www.our-internet.org/report> [Erişim 3 Ekim 2016].
- 15 Wiener N (1948) Cybernetics: Or Control and Communication in the Animal and the Machine.

- 16 Gibson W (1984) Neuromancer. New York: Ace Books.
- 17 Newitz A (2013) The bizarre evolution of the word 'cyber'. <http://io9.gizmodo.com/ today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487> [Erişim 3 Ekim 2016].
- 18 European Commission (2015) A Digital Single Market Strategy for Europe. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192> [Erişim 11 Ekim 2016].
- 19 Cited in Helfand D (2001) Edpseak is in a class by itself. Los Angeles Times, 16 Ağustos. <http://articles.latimes.com/2001/aug/16/news/mn-34814> [Erişim 3 Ekim 2016].
- 20 Bu kısım, modern yönetim meseleleri konusundaki "muhalif" görüşleri Diplo'nun öğretim ve araştırma faaliyetlerinde sabit bir gerçeğe uygunluk teşkil eden Diplo'nun kıdemli yetkilisi Aldo Matteucci ile görüşmeden tamamlanamamıştır.
- 21 United Nations General Assembly (2015) Resolution A/70/125. Bilgi Toplumu konusundaki Dünya Zirvesinin çıktılarının uygulanmasının gözden geçirilmesine ilişkin Genel Kurul sonuç dokümanı. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf> [Erişim 10 Ekim 2016].
- 22 NATO (2016) Warsaw Summit Communiqué. http://www.nato.int/cps/en/natohq/official_texts_133169.htm [Erişim 10 Ekim 2016].
- 23 Broeders D (2015) The public core of the Internet. Amsterdam: Amsterdam University Press. http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf [Erişim 3 Ekim 2016].
- 24 Büyükelçi Trigona'nın BM Genel Kurulunun New York'ta World Summit on Information Society Review Process'e adanan 15 Aralık 2015 tarihindeki toplantısında yaptığı konuşma <https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf> [Erişim 3 Ekim 2016].
- 25 WSIS süreci Temmuz ayında Cenevre'de yapılan ilk hazırlık toplantısı ile başlamıştır. İlk zirve Cenevre'de (Aralık, 2003), ikinci zirve ise Tunus'ta düzenlenmiştir (Kasım, 2005).
- 26 Volker Kitz telefon sistemlerinin idare edilişi ile İnternet isimleri ve sayıları arasında bir analogi ileri sürmüştür. Kitz V (2004) ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called 'uniqueness' of the Internet. <http://studentorgs.law.smu.edu/Science-and-Technology-Law-Review/Articles/Fall-2005/Kitz.aspx> [Erişim 16 Ekim 2012].
- 27 US Supreme Court (1997) Decision in Reno vs American Civil Liberty Union. <https://supreme.justia.com/cases/federal/us/521/844/case.html> [Erişim 10 Ekim 2016].
- 28 Alıntı: Mock K, Armony L (1998) Hate on the Internet. <http://www.bnaibrith.ca/league/hoti/hoti-00.html> [Erişim 20 Ekim 2012].
- 29 Alıntı: Mock K, Armony L (1998) Hate on the Internet. <http://www.bnaibrith.ca/league/hoti/hoti-00.html> [Erişim 20 Ekim 2012].
- 30 "Basket (boyut)" terimi Avrupa Güvenlik ve İşbirliği Teşkilatı (OSCE) müzakereleri esnasında diplomatik uygulamaya geçmiştir.
- 31 CSTD (2015) Mapping of international Internet public policy issues. http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf [Erişim 19 Ekim 2016].

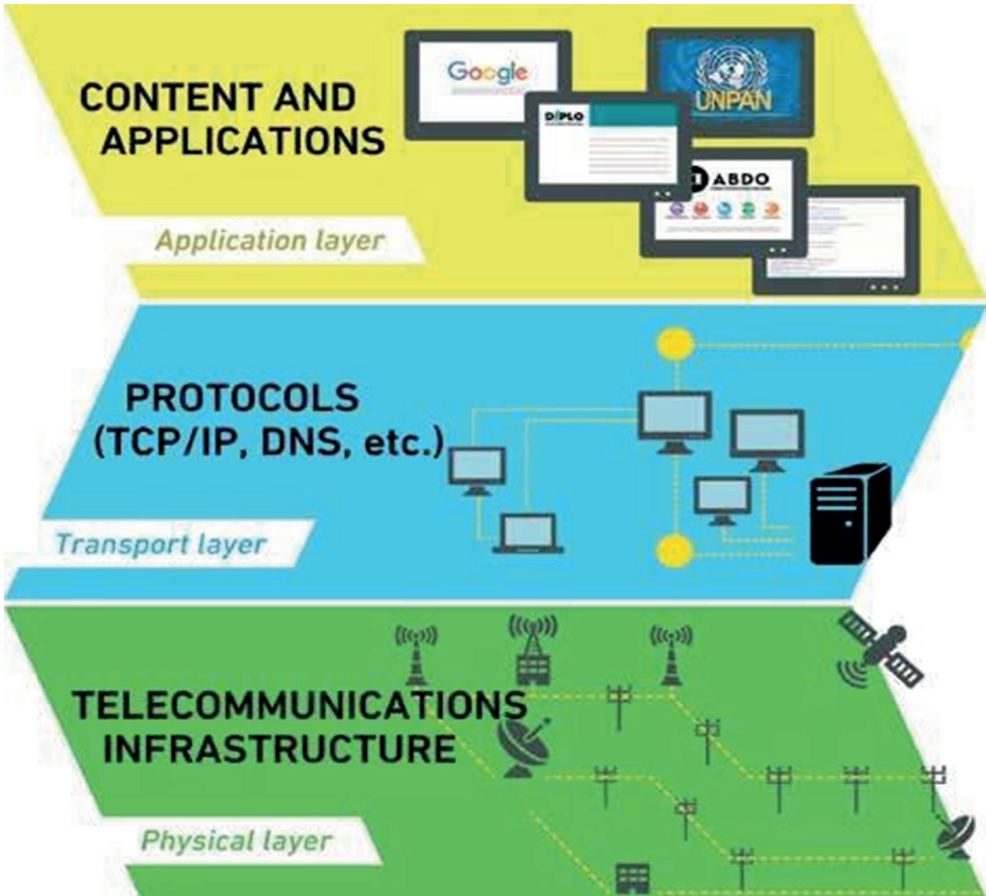
Bölüm - 2

Altyapı Sepeti

ALTYAPI SEPETİ

Altyapı sepeti, İnternet ile ilgili daha çok teknik içerikli temel konuları kapsamaktadır. Bir konunun, bu gruba dâhil edilebilmesi için gerekli temel kriter, konunun İnternetin, çalışması ve işleyişi ile ilgili olmasıdır. Bu sepet, eksiklikleri halinde İnternet ve World Wide Web'in (www)¹ var olmasının mümkün olmayacağı temel konuları kapsar. Bu konular bir ölçüde aşağıda Şekil 5'de görüldüğü üzere üç-katmanlı internet modelini izleyen üç temel gruba bölünmektedir:

- 1 İnternet trafiğinin aktığı telekomünikasyon altyapısı.
- 2 İnternete ilişkin (teknik ve web standartları gibi) standartlara ve (IP, DNS ve kök bölgesi gibi) kritik internet kaynaklarına ilişkin teknik konular.
- 3 Ağ tarafsızlığı, bulut hesaplaması, nesnelerin internet ve çakışma gibi birbirini kesen konular.



Şekil 5. İnternet katmanları

Telekomünikasyon altyapısı²

Mevcut durum

İnternet içinde trafiğin aktığı bir araç olarak telekomünikasyon altyapısını kullanır: bakır veya fiberoptik tellerden oluşan kablolar; uydular, kablosuz bağlantılar ve mobil ağlar gibi elektromanyetik dalgalar gibi. Pek çok durumda telefon hatları ve mobil bağlantılar, enerji nakil hatları³, denizaltı kabloları veya uydu bağlantısı gibi var olan telekomünikasyon altyapısı internet paketlerini taşımak için kullanılır. Giderek artan şekilde taşımak üzere nesnelerin internetini daha fazla yaymaya yarayacak teknolojiler kadar yüksek bant denizaltı fiber optik kabloları, beşinci nesil mobil ağlar ve Google balonları⁴ veya Televizyon Beyaz Alanları⁵ gibi yaratıcı yenilikçi çözümler gündeme gelmektedir.

En sık kullanılan internet bağlantı teknolojileri

Kablolu telekomünikasyon altyapısı

- Dijital abone hatları (DSL): veri ve ses trafiğini iletmek için mevcut bakır telefon kablolarını kullanır.
- Televizyon kablo ağları: kablo geniş bant hizmetleri, kablolu televizyon altyapısı üzerinden İnternete erişim sağlar.
- Fiber optik: Optik fiber ağlar, İnternet'in tercih edilen omurga altyapısıdır, çünkü tek bir fiber, mesafeden belirgin bir sinyal bozulması olmadan, çok uzak mesafelerde önemli miktarda veri taşıyabilir.
- İnternet üzerinden güç hatları: kullanıcıların bir cihazı herhangi bir elektrik prizine takmalarını ve anında yüksek hızlı İnternet hizmeti almalarını sağlar.

Kablosuz telekomünikasyon altyapısı

- Uydu İnternet: Karasal İnternet erişiminin mümkün olmadığı yerlerdeki topluluklara ve sıkça hareket eden topluluklara İnternet bağlantısı sağlamak için kullanılır.
- Wi - Fi: cihazların kablosuz yerel alan ağlarına (WLAN) radyo frekansları üzerinden bağlanmasına izin verir.
- WiMAX (Mikrodalga Erişimi için Dünya Çapında Birlikte Çalışabilirlik): lisanslı ve lisanssız frekansları kullanarak kablo ve DSL'ye alternatif olarak uzun mesafelerde kablosuz genişbant erişimi sağlamayı kolaylaştırır.
- Mobil geniş bant: En yaygın kullanılan teknolojilerden biri, Avrupa'da ortaya çıkan ve üçüncü ve dördüncü nesil (3G ve 4G) ile küresel olarak baskın hale gelen nihayetinde 5G olan ve özellikle dünyaya hakim hale gelen Mobil İletişim için Küresel Sistemdir (GSM).

Telekomünikasyona ilişkin düzenlemeler İnternet yönetişimini doğrudan etkileyecektir. Telekomünikasyon altyapısı, ulusal ve uluslararası düzeylerde düzenlenmektedir. Telekomünikasyonun düzenlenmesine dâhil olan belli başlı uluslararası örgütler ulusal telekomünikasyon sis-

temleri, radyo frekans dağılımı ve uydu konumlandırma yönetimi arasındaki koordinasyon için kurallar geliştiren kurum olan Uluslararası Telekomünikasyon Birliği (ITU) ve dünya çapında telekomünikasyon piyasalarının serbestleştirilmesinde temel rolü üstlenen kurum olan Dünya Ticaret Örgütü (WTO) olmaktadır⁶.

Uluslararası Telekomünikasyon Düzenlemesi

1988 ITU'nun ITR'leri, uluslararası fiyatlandırma ve hizmetlerin serbestleştirilmesini kolaylaştırdı ve Internet alanında uluslararası kiralık hatlar gibi temel hizmetlerin daha yenilikçi bir şekilde kullanılmasına olanak sağlamıştır. ITR'ler 1990'lı yıllarda İnternetin hızlı büyümesi için altyapılardan birini sağlamıştır. ITR'ler Aralık 2012'de Dubai'de düzenlenen WCIT 12 değiştirilmiştir; çoğu gelişmekte olan ülke konumundaki 89 ülke değiştirilen ITR'leri imzalarken, ABD ve birçok Avrupa ülkesi de dahil olmak üzere 55 ülke imza atmıştır⁷. Böylece, 1 Ocak 2015'ten başlayarak 2012 ITR'leri devreye girdiğinde iki uluslararası telekomünikasyon rejimi (1988 ve 2012 yılları arasında) faaliyet göstermekteydi. Bereket versin ki, 2012'deki değişiklikler önemli olmadığı için, küresel telekomünikasyon sisteminin bütünlük işlevselliğini etkilememiştir. Ancak, bu "yönetişim ikiliği" çözülmesi gereken bir şey olarak ortada durmaktadır.

ITU ve WTO'nun rolleri oldukça farklıdır. ITU gönüllülük esasıyla teknik standartları ve telekomünikasyona özgü uluslararası yönetmelikleri belirler ve geliştirmekte olan ülkelere destek sağlar.⁸ Politika tartışmalarının birçoğu, VoIP, siber güvenlik ve dijital nesne tanımlayıcıları (Dijital Nesne Mimarisi - DOA)⁹ gibi telekomünikasyon altyapısı ile İnternet arasındaki sınırda olan politika sorunlarıyla ilgilenen ITU ile ilgilidir. WTO ise genel piyasa kuralları için bir çerçeve hazırlar.¹⁰ Telekomünikasyon alanındaki rolü bugüne kadar herhangi bir büyük tartışmaya yol açmamıştır. Bununla birlikte, WTO'nün e-ticarete daha aktif katılımı, e-ticaret ile siber güvenlik ve veri koruma gibi ilgili alanlar arasındaki sınıra ilişkin tartışmaları tetikleyebilir.

Meseleler

İnternet omurga kabloları¹¹

İlk telgraf kablosu 1870 yılında Hindistan'a Akdeniz, Kızıldeniz ve Hint Okyanusu üzerinden ulaştığından beri, çoğu uluslararası elektronik iletişim trafiği deniz dibi kablolarıyla taşındı. Şu anda, tüm küresel İnternet trafiğinin% 90'ından fazlası telgraf tarafından kullanılan eski coğrafi rotaları büyük ölçüde takip eden denizaltı fiber optik kablolarından geçmektedir.

Denizaltı İnternet kabloları birkaç İnternet trafiği merkezinde karaya ulaşır. Latin Amerika'nın çoğu kabloları Miami'de karaya ulaşır. Asya'da, kilit İnternet trafiği merkezleri Singapur ve Hong Kong'tur. İnternet trafiğinin diğer önemli noktaları arasında Amsterdam, New York ve San Francisco bulunmaktadır. İnternet kabloları ve trafiği için en savunmasız noktalar, Luzon, Hürmüz ve Malacca Boğazları ile Süveyş Kanalı gibi geleneksel stratejik sıcak noktalar olmaya devam etmektedir.

Asya ve Avrupa arasındaki dijital bağlantıda, coğrafya da önemlidir. Örneğin, Asya ve Avrupa arasındaki İnternet trafiğinin % 95'i, Süveyş Kanalı'nı kısayol olarak kullanan deniz taşımacılığına benzer şekilde Mısır'dan geçmektedir.

İnternet trafiğinin çoğu şu anda denizaltı kablolarından geçtiğinden, yeni karasal İnternet kablolarının kurulumu, özellikle Asya ve Avrupa arasındaki İnternet trafiğinin çeşitlendirilmesinde önemli bir adım olarak görülmektedir.

Birleşmiş Milletler Asya ve Pasifik Ekonomik ve Sosyal Komisyonu (UNESCAP) ve Asya Kalkınma Bankası, 141.000 km'lik kıtalararası bir ulaşım altyapısı projesi olan Asya Otoyolunun dijital bir bileşenini desteklemektedir.¹² Ayrıca, Trans-Eurasian Enformasyon Süper Otoyolu (TASIM), iki kıta arasındaki veri akışını daha da çeşitlendirecek şekilde Doğu Avrupa ve Orta Asya'yı birbirine bağlamayı planlamaktadır. Proje "Doğu Asya ortakları ile bağlantının hızını ve İnternetin esnekliğini arttırmayı" ve bu süreçte Orta Asya'daki bölgesel işbirliğini geliştirmeyi amaçlamaktadır.¹³

Dijital bakış açıları aynı zamanda, Dijital İpek Yolu olarak adlandırılan dijital bir bileşeni içeren Tek Kemer, Tek Yol girişiminde belirgin bir özelliğe sahiptir.¹⁴ Dijital bağlantı, demiryolları ve enerji botu hatları boyunca fiber optik kabloların döşenmesini içerecek olan ulaşım ve enerji altyapısı projelerinden faydalanabilir.

Planlanan tüm karasal kablo projeleri ve özellikle Dijital İpek Yolu, tarihte ilk defa, önemli ölçüde bir telekomünikasyon trafiğini deniz tabanından karasal kablolarla kaydırmaktadır.

Yerel ağın paylaşıma açılması

"Local loop" (veya "last mile") İnternet Servis Sağlayıcılar (ISP'ler) ile bunların bireysel müşterileri arasındaki bağlantıya verilen isimdir. Yerel ağ ile ilgili (kötü durumdaki kablo hatları, güç kayıpları vb gibi) sorunlar, daha çok gelişmekte olan ülkelerde İnternetin daha yaygın kullanımı için bir engel teşkil etmektedir. Yerel ağın paylaşıma açılması sorunu için mümkün olan ve düşük maliyetli tek çözüm kablosuz iletişimdir. Son yıllarda, Google, balonlardan (Project Loon) kablosuz mobil erişim sağlama konusunda deneme yaparken, Facebook bir dron filosu kullanarak İnternet erişimi sağlama üzerinde çalışmaktadır. Gittikçe artan mevcut teknolojik seçenekler dışında yerel ağın paylaşıma açılması sorununun çözümü birden fazla işleticinin (yerel ağın ayrı fiyatlandırılması süreci olarak bilinen) telefon ağ paylaşımını kullanmasına imkan sağlanması da dahil telekomünikasyon piyasasının bu segmentinin serbestleşmesine bağlıdır.

Telekomünikasyon piyasalarının serbestleşmesi

Tarihsel olarak telekomünikasyon altyapısı ve hizmetleri devlete ait işletmeciler tarafından tekel olarak temin edilmiştir. Son yirmi yılda pek çok ülke, telekomünikasyon sektörünü serbestleştirmiş ve yeni işletmecilerin piyasaya girmesine ve rekabetçi şekilde iletişim ağ ve hizmetlerini sağlamalarına izin vererek piyasayı rekabete açmıştır. Serbestleştirme ayrıca yeni servis sağlayıcılarına (devletin sahip olduğu) mevcut altyapıya ulaşma imkanı verilmiş olması anlamına da

gelmektedir. Devlete ait iletişim işletmelerinin özelleştirilmesi de serbestleştirme politikalarına paralel seyretmiştir. Ancak, bu süreç gelişmekte olan ülkeler arasında daha yavaş seyretmektedir. Bu ülkeler genellikle bir taraftan telekomünikasyon piyasasını serbestleştirip daha verimli bir hale getirmek ve diğer taraftan mevcut telekomünikasyon tekellerini (özellikle, geleneksel telefonun uluslararası düzenini sürdüren yapısından keyif aldıkları bir şey olarak) önemli bütçe gelir kaynağı sağladıkları için korumak ikilemi ile karşı karşıya kalmaktadır. WCIT - 12’de ve diğer uluslararası toplantılarda bazı gelişmekte olan ülkeler tarafından ileri sürülen bu tür finansal kaygılar, ortaya çıkan İnternet iletişim hizmetlerinden elde edilen gelirlerin yeniden dağıtılması sorusunu ortaya çıkarmıştır.

Elektromanyetik spektrum yönetimi

Kablosuz iletişim genellikle kablolu bir altyapının kullanımına daha uygun bir alternatif olarak görülmekle birlikte, spektrumun uygunsuz özelliklerinden biri de, bunun sınırlı olmasıdır. Teorik olarak, her bir frekans segmentini sonsuz küçük parçalara bölebilirsiniz, ancak pratikte kullandığımız ekipman (spektrumu daha verimli kullanmak için sürekli geliştirilse bile) kullanılabileceği frekans bantlarının darlığı ile sınırlıdır ve aynı frekansı kullanan diğer aygıtlarla çakışmaması gerekir. Bu, bir veya daha fazla tipte radyo iletişim servisinin kullanımı için belirli frekans bantlarını tahsis etmenin yanı sıra, spektrumun belirli bölümlerini TV istasyonları, radyo yayıcıları, mobil ağ işletmecileri, internet servis sağlayıcıları dahil olmak üzere belirli kesimlere tahsis için bir yetkili olması gerektiğine işaret etmektedir.

Her ülkedeki frekans yönetimi (yani hangi teknolojilerin ve hangi hizmet sağlayıcıların tahsis edilen spektrumun hangi alt segmentini ve hangi lisanslarla kullanılabileceğine dair kararlar) genellikle kendi ulusal tahsislerini komşu ve diğer ülkeler iki taraflı olarak veya (AB’nin Radyo Spektrum Komitesi (RSC) ve Radyo Spektrum Politika Grubu (RSPG) gibi) bölgesel inisiyatiflerle veya (ITU gibi) uluslararası kurumlar ile daha da uyumlu hale getiren telekomünikasyonu düzenleyen ulusal makamların elindedir.

ABD’de ve çoğu AB üye devletinde olduğu gibi, örneğin, radyo frekanslarını kullanma haklarının verilmesi, frekansları açık artırma işlemlerine sunarak yapılır. AB, üye devletler arasında radyo frekanslarının kullanımında bir miktar uyumlaştırma sağlamak amacıyla, radyo spektrum yönetimi için kapsamlı bir düzenleyici yaklaşım geliştirmiştir.¹⁵ Spektrumun belirli bölümlerinin kullanımına lisans verilmesi ve bunun için (mobil ağ işletmecileri gibi) en fazla ödeyene tahsis edilen spektrumun belirli ihtiyaçlara göre kullanılmasını sağlar, ayrıca devletlere de iyi gelir sağlar.

En yaygın olarak kablosuz geniş bant ve mobil iletişim olan radyo spektrumunu kullanan yeni iletişim hizmetlerinin geliştirilmesi, dünyanın dört bir yanındaki hükümetleri optimal spektrum kullanımına uygun çözümler bulmaya teşvik ederek radyo frekanslarına olan talebi artırdı. Dijital iletişim için kullanılabilir spektrum bandını genişletmenin bir yolu, analog TV yayıncıları tarafından kullanılan geniş spektrumun bir kısmını serbest bırakmaktır: yayın şirketlerini analog sinyalden (her bir haneye ek cihazlar konulması kadar yeni yayın ekipmanlarına da ciddi yatırım yapmayı gerektiren fakat daha iyi hizmet kalitesi ve diğer hizmetler için fırsatlar sunan) dijital sinyale dönmeye motive ederek, spektrumun önemli kısmının (dijital hisse olarak adlandırılan) diğer hizmetlere ayrılması mümkün olabilecektir.

Spektrum kullanımının hacmi ve sınırları teknolojik gelişmelerden etkilenir. Bu, bazı gruplar tarafından ileri sürülen, mevcut hükümet düzenlemelerinin (bir eve veya başka bir mekana Wi-Fi kurmak için lisans gerekmediği anlamına gelen) sıradan Wi-Fi için kullanılan lisanssız yaklaşımı izleyecek olan herkese açık erişim demek demek olan ‘açık spektrum’ ile değiştirilmesi gerektiği yönündeki argümanı ortaya çıkarmıştır. Bununla birlikte, bu görüşle ilgili iki potansiyel sorun bulunmaktadır. Bunlardan biri, özellikle Avrupa’daki telekomünikasyon şirketlerinin 3G ve 4G mobil telefon şebekelerini kullanma haklarını elde etmek için yaptığı dev yatırımlarla ilgilidir. Açık bir spektrum politikası bu şirketler için haksızlık olur. Telekomünikasyon sektöründe iflas ve istikrarsızlıklarını tetikleyebilir. Diğer, eğer spektrum tüm kaynaklar için serbestse, bu bunun pek çok kişinin faydalanabileceği bir kamusal mal olarak kullanılması gerektiği anlamına gelmez. Bu, daha ziyade, öncelikle “serbest” spektrumdan, kâr dahil, kendi amaçları için yararlanabilecek teknik kapasiteye sahip aktörler tarafından kullanılabilir.

ISP’ler

İnternet erişim mimarisi üç katmandan oluşmaktadır. Son kullanıcıları birbirine bağlayan ISS’ler, 3. katmanı oluşturur. 1. ve 2. katmanlar, İnternet bant genişliği sağlayıcılarından (IBP’ler) oluşur. 1. katman başlıca IBPlerin taşıyıcısıdır. 1. ve 2. katman arasındaki temel fark 1. katman IBP’lerinin değiş tokuş ile trafiği takas etmesi¹⁶ ve 2. katman IBP’lerin 1. katman sağlayıcılarına transit geçiş ücreti ödemek zorunda olmasıdır.¹⁷ 1. katman genellikle AT&T, Verizon, Level 3 Communication, Vodafone ve NTT Communications gibi büyük şirketler tarafından yönetilir.

Meseleler

Telekomünikasyon tekelleri ve ISP’ler

Telekomünikasyon tekelleri olan ülkelerde, bu tekellerin İnternet erişimi de sağlaması yaygındır. Tekeller, diğer ISP’lerin bu pazara girmesini ve rekabeti engellemektedir. Bu, daha yüksek fiyatlar ve genellikle daha düşük hizmet kalitesi(QoS)’yle sonuçlanmakta ve dijital uçurumun azaltılması çabalarını başarısız kılmaktadır. Bazı durumlarda, telekomünikasyon tekelleri diğer ISS’lerin varlığını tolere etmekte, ancak (örneğin daha düşük bant genişlikleri sağlayarak veya hizmetlerde aksamalara neden olarak) operasyonel düzeyde müdahale bulunmaktadır.

Telekomünikasyonun serbestleşmesi ve ISP’lerin ve IBP’lerin rolü

ISP’lerin ve IBP’lerin mevcut uluslararası araçlara ne ölçüde tabi olacağı konusunda birbirine zıt görüşler bulunmaktadır. Esas olarak gelişmiş ülkeler tarafından paylaşılan bir görüş, DTÖ’nün telekomünikasyon işletmecilerine verdiği serbesti kurallarının aynı zamanda ISP’lere de genişletilebileceğini savunmaktadır. Genel olarak gelişmekte olan ülkelere bazıları da, DTÖ telekomünikasyon rejiminin sadece telekomünikasyon piyasası için geçerli olduğunu savunmaktadır. Bu görüşe göre, ISS pazarının düzenlenmesi yeni DTÖ kuralları gerektirmektedir.

ISP'lerin yasal kuralların uygulanmasındaki rolü

ISP'ler son kullanıcıları İnternete bağladıklarından, İnternet üzerinde yasal kuralların en doğrudan ve açık şekilde uygulanmasını sağlayabilir görünmektedirler. Bu nedenle birçok devlet, telif hakkı ihlali, çevrimiçi çocukların korunması ve diğer içerik politikası gibi alanlarda kanun uygulama çabalarını ISP'ler üzerine yoğunlaştırmaya başlamıştır.

Aracıların rolü konusunda daha fazla tartışma için Bölüm 4'e bakınız.

İnternet altyapısı bir kamu hizmeti olarak düşünülmeli midir?

İnternet verileri herhangi bir telekomünikasyon ortamı üzerinden akabilir. Uygulamada, genellikle optik kablolar veya uydu bağlantılarına sahip olan 1. katman omurgaları gibi imkanlar (yani, İnternet'te büyük, stratejik olarak birbirine bağlı ağlar ve çekirdek yönlendiriciler arasındaki temel veri yolları gibi) İnternetin işletilmesinde kritik hale gelmiştir. İnternet ağı içerisindeki temel konumları, 1. katman sahiplerine hizmetlerini sunarken fiyatları ve şartları belirleyecek piyasa gücü sağlar.¹⁸ Sonuçta, İnternetin işleyişi, merkezi omurga sahiplerinin aldığı kararlara bağlı olabilir. Veri hacmi akışlarındaki artış eğilimi, aslında telekomünikasyon sektörüyle doğrudan bağlantısı olmayan bazı yeni oyuncularını da beraberinde getirmiştir. Örneğin, Google, Facebook ve Microsoft, son yıllarda kendi denizaltı kablolarının yerleştirilmesini finanse etmeye başlamıştır.¹⁹

İnternetin güvenilirliği garanti edilebilir mi?

Küresel İnternet topluluğunun kritik İnternet altyapısının büyük İnternet şirketlerinden ve telekomünikasyon operatörlerinden güvenilir bir şekilde çalışması için güvence ve garanti talep etmesi mümkün müdür?

Şu anda, böyle bir durum yoktur. Bununla birlikte, eğilim özel internet altyapısı operatörlerine bazı kamu gereksinimlerini empoze etme yönünde görünmektedir.

IBP'ler ve kritik altyapı

2008'in başlarında, ana internet kablolarından birinin Mısır yakınlarındaki Akdeniz'de kopmasıyla bir kesinti meydana geldi. Bu olay, Hindistan'a kadar uzanan geniş bir bölgedeki internete erişimi tehlikeye soktu. Tayvan ve Pakistan yakınındaki İnternet kablolarında meydana gelen benzer iki olay, İnternet altyapısının ulusal ve küresel bir kritik altyapının parçası olduğunu açıkça göstermiştir. İnternet hizmetlerinin bozulması, genel ekonomiyi ve bir bölgenin sosyal yaşamını etkileyebilir. Bu tür bir kesinti olasılığı bir dizi soruyu beraberinde getirmektedir:

- Ana İnternet kabloları uygun şekilde korunuyor mu?
- Ulusal hükümetlerin, uluslararası kuruluşların ve özel şirketlerin İnternet kablolarının korunmasındaki görel rolleri nelerdir?

- Ana İnternet kablolarının bozulması ihtimali ile ilgili riskleri nasıl yönetebiliriz?

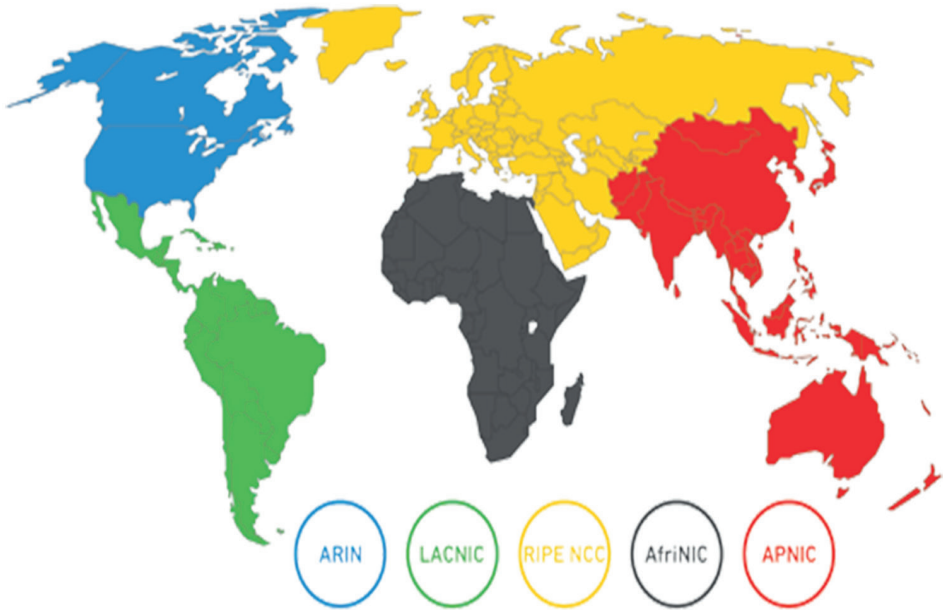
www.igbook.info/infrastructure

İletişim Kontrol Protokolü(TCP) / İnternet Protokolü(IP)

Mevcut Durum

TCP/IP, İnternetin temel teknik standardıdır. Üç prensibe dayanır:

- **Paket - aktarma:** Mesajlar paket adı verilen küçük parçalara ayrılır ve İnternet üzerinden farklı yollardan ayrı olarak gönderilir, alıcı tarafındaki orijinal mesaja tekrar monte edilir.



Şekil 6.Bölgesel İnternet Kütükleri

- **Uçtan uca ağ iletişimi:** Bu, iletişim işlemlerinin ve hizmetlerinin kaynak ve alım noktalarında gerçekleşmesi gerektiğini belirtirken, ağ kendisinin mümkün olduğu kadar tarafsız veya 'dilsiz' olması gerektiğini belirten temel tasarım ilkelerinden biridir.
- **Sağlamlık:** Veri gönderme, özelliklere uygun olmalı, diğer taraftan uygun olmayan bilgileri kabul edebilmek için veri alımı daha esnek olmalıdır.

TCP/IP'ye ilişkin internet yönetişi iki önemli boyuta sahiptir:

- Yeni standartların oluşturulması.
- IP numaralarının dağıtılması.

TCP/IP standartları, İnternet Mühendisliği Görev Gücü (IETF) tarafından belirlenir. Bu protokollerin asıl ilişkisi İnternet ile olduğundan IETF tarafından titizlikle ve sürekli gözden geçirilirler. TCP/IP'deki herhangi bir değişiklik, kapsamlı bir tartışma ve etkili bir çözüm olduklarının kanıtını gerektirir (örn. 'çalışan kod' ilkesi).

Bir **IP adresi (veya numarası)**, İnternete bağlı her cihazın sahip olması gereken benzersiz bir sayısal adrestir; her adres, İnternet yönlendirme sistemi aracılığıyla bir ağ konumuna nasıl erişileceğini belirtir. Genel olarak, İnternete bağlı iki cihaz aynı IP adresine sahip olamaz.

IP numaralarının dağıtım sistemi hiyerarşik olarak düzenlenmiştir. En üstte, işlevleri şu anda PTI tarafından gerçekleştirilen bir ICANN üyesi olan IANA'dır.²⁰ PTI, IP sayı bloklarını beş bölgesel İnternet kütüğüne (RIR) dağıtır (Şekil 6).²¹ RIR, IP numaralarını yerel İnternet kütüklerine (LIRs) ve ulusal internet kütüklerine (NIRs) dağıtır. Buna karşılık NIR'ler de IP numaralarını daha küçük İSS'lere, şirketlere ve daha alt katmanlardaki bireylere dağıtır.

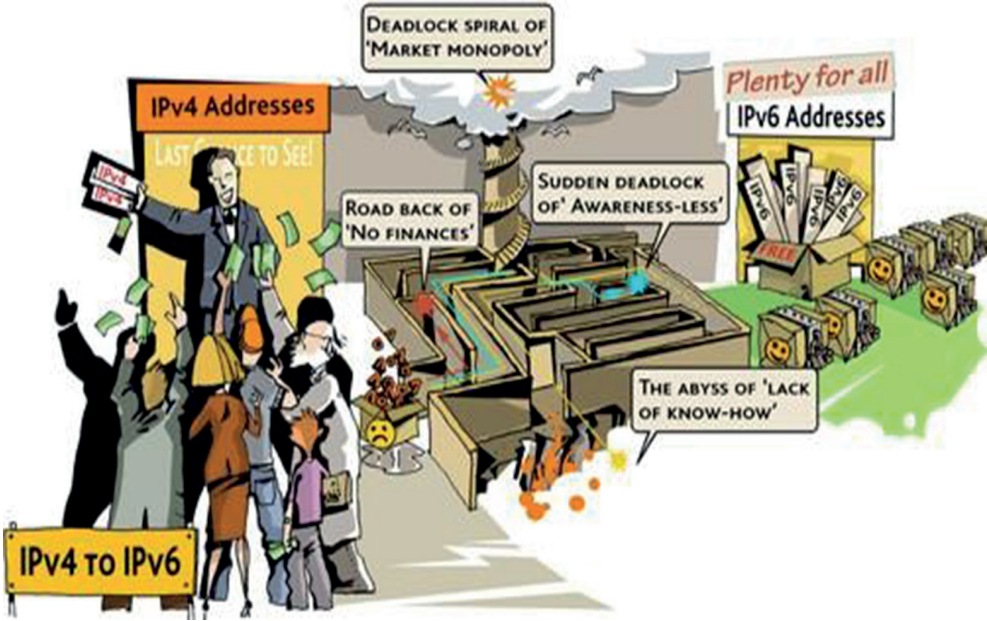
Meseler

IP numaralarının sınırlılıkları ve IPv6'ya geçiş

1983'te tanıtılan IP sürüm 4 (IPv4) altındaki IP numaralarının havuzu, başlangıçta adreslerin talebini karşılamak için yeterli olduğu düşünülen dört milyar rakamı içermektedir. Ancak, Şubat 2011'de IANA, artık RIR'lere tahsis edilecek IPv4 blokları olmadığını açıkladı.

IPv4 sayılarının eksilmesi, İnternet özellikli cihazların (cep telefonları, akıllı cihazlar, oyun konsolları ve ev aletleri gibi) ortaya çıkması ve dünya çapında İnternet bağlantısının artmasıyla son yıllarda hızlanmıştır. İnternette IP adreslerine ihtiyaç duyan NesNet cihazları ile birlikte NesNet alanındaki gelişmeler de IP adreslerine olan talebin artmasına neden olmuştur. IP numaralarının tükenmesi ve sonunda İnternet'in daha da gelişmesini engellemesi endişesi teknik topluluğun üç önemli önlem almasına neden olmuştur.

- Ağ Adresi Çevirisi (NAT) ortaya çıkması ile mevcut IP numaraları havuzunun kullanımını rasyonelleştirmek: özel bir ağdaki bilgisayarların (şirketler ve kuruluşlarda kullanılanlar gibi) bağlantı yaparken tek bir IP adresini paylaşmalarına izin veren bir teknik.
- Daha önce Sınıfsız Alanlar Arası Yönlendirmenin (CIDR) ortaya çıkmasıyla RIR'ler tarafından daha önce kullanılan savurgan adres tahsisi algoritmaları belirlemek: Çok basit bir ifadeyle, tek bir IP adresinin birçok benzersiz IP adresi belirleyebilmesine izin veren (böylece IP adres tahsisini daha verimli hale getiren) bir IP adres şeması.
- Çok daha büyük bir IP numarası havuzu (340.000.000.000.000.000'den fazla) sağlayan yeni bir IP sürümü olan IP sürüm 6'nın (IPv6) ortaya çıkması.



Şekil 7. IPv4 to IPv6

İnternet teknik topluluğu proaktif bir şekilde IP numaralarının olası bir kıtlığı sorununa cevap vermiştir. NAT ve CIDR problem için hızlı bir çözüm sağlarken, uygun bir uzun vadeli çözüm IPv6'ya geçiş olmuştur.

Bununla birlikte, IPv6 1996 yılında ortaya çıkmış olsa da, geçiş ihtiyacı konusunda farkındalığın yanı sıra, gelişmekte olan ülkelerde yeni ekipmanlara yapılan yatırım için sınırlı fonları nedeniyle konuşlandırılması yavaş olmuştur (Şekil 7). Uzmanlar, IPv6'ya yavaş bir geçişin, IPv4 ve IPv6 şeklinde iki paralel internetin birbiriyle etkileşemeyeceğinden yola çıkarak İnternet'in sözde teknik parçalanmasına yol açma riskleri konusunda uyarılarda bulunmuşlardır. Örneğin, 2016'nın başında WEF²² tarafından yayınlanan ve İnternet'in sadece % 4'ünün IPv6 kullanımına hizmet ettiği bir raporunda, bunun altı çizilmiştir.

İnternet teknolojisi, IPv4 ve IPv6'nın bir arada bulunmasına izin vermektedir; IPv6 kullanan çoğu ağ, hem IPv4 hem de IPv6 adreslerini desteklemektedir. Bununla birlikte, iki protokol arasında sorunsuz geçiş için, doğru İnternet çalışması, bir arada bulunma, kolay adres eşleme ve ad hizmeti geçişinde mekanizmalar uygulamak için bir dizi teknik gerekmektedir. IPv6 için IETF spesifikasyonları ilgili geçiş stratejileri, araçları ve mekanizmaları içermektedir.²³

Geçiş probleminin yanı sıra, IPv6 dağıtımına ilişkin politika çerçevesi, son kullanıcıların ihtiyaçlarını en iyi şekilde ele almak için açık ve rekabetçi mekanizmaların kullanılmasını talep ederek IP numaralarının uygun bir şekilde dağıtılmasını gerektirecektir. IPv6'nın ortaya çıkmasıyla bile, ISS'ları gibi bunları yerel düzeyde dağıtmaktan sorumlu olanların güçlerini kötüye kullanmayı seçmeleri ve bu tahsis örneğinin, diğer hizmetlerin satın alınmasıyla ilişkilendirmele-

ri, böylece IP numaralarının mevcudiyeti ve fiyatını etkilemeleri halinde “yapay” bir IP kıtlığı var olmaya devam edecektir.

IPv4’ten IPv6’ya geçiş, geniş bir paydaş yelpazesinin katılımını gerektirir. IANA / PTI, RIR’ler ve IETF gibi teknik kuruluşların IPv6 kaynaklarının etkin ve etkin bir şekilde yönetilmesi ni sağlamaları ve IPv6 kullanımı için gerekli standartları ve özellikleri geliştirmeleri gerekir. ISS’ler, IPv4 ve IPv6 arasında iletişimi sağlayan teknikleri uygulamak ve ağlarına ve hizmetlerine IPv6’yı tanıtmak zorundadır. Ekipman üreticilerinin (işletim sistemleri, ağ ekipmanı vb.) ve uygulama geliştiricilerinin (işletme yazılımı, akıllı kartlar, vb.) ürünlerinin ve uygulamalarının IPv6 ile uyumlu olmasını sağlaması gerekir. Bilgi toplumu hizmet sağlayıcıları IPv6’yı kendi sunucuları içinde uygulamak zorundadır.²⁴

TCP/IP’deki Değişiklikler ve Siber güvenlik

İnternet (1970-1980’de) kapalı bir araştırma kurumları ağından oluşurken İnternet’in orijinal geliştiricileri için güvenlik önemli bir sorun değildi. İnternetin dünya çapında üç milyar kullanıcıya yayılması ve ticari ve toplumsal bir altyapı olarak artan önemi ile birlikte, internet yönetimi sorunları listesinde güvenlik sorunu oldukça yüksek bir noktaya gelmiştir.

IPv4, IP güvenlik desteği (IPSec olarak da bilinir) sunsa da, bu özellik isteğe bağlıdır. IPv6’da güvenlik gereklidir ve IPSec, herhangi bir uygulamayı ayarlamak zorunda kalmadan İnternet trafiğinin kimlik doğrulama, şifreleme ve sıkıştırılmasını sağlayan ayrılmaz bir parçası olmuştur.²⁵

IPv6, IPv4 ağlarını etkileyen, aygıt kimlik doğrulaması, veri bütünlüğü ve gizlilik dahil olmak üzere bilinen güvenlik açıklarını gidermektedir. Her ne kadar IPv6 bu durumlarda daha iyi güvenlik sunsa da, protokol aynı zamanda, daha basit IPv4’den daha muhtemel olan kötü uygulama ve yanlış yapılandırma nedeniyle bazı yeni güvenlik problemlerini de beraberinde getirmektedir.²⁶ Bu endişelerin çoğu, dikkatli geçiş prosedürleriyle hafifletilebilir, ancak bu konulardan duyulan korku, farkındalık eksikliği ve düşük öncelik pek çok işletmenin IPv6’ya geçişi geciktirmesine neden olmaktadır.²⁷

Ek olarak, bağlanan her cihaza benzersiz bir tanımlayıcı atanacağı için IPv6 adreslerinin gizliliği engelleyebileceği endişeleri bulunmaktadır. Bununla birlikte, bu tanımlayıcının statik kalmasına gerek yoktur, ancak dinamik olarak atanabilir ve ara sıra değiştirilebilir; Bu nedenle, IPv6’nın uygulanma şekli bu konuda önemli olacaktır.

TCP/IP’deki değişiklikler ve sınırlı bant genişliği sorunu

Multimedya içeriğinin (örneğin, İnternet telefonu veya isteğe bağlı video gibi) yayınlanmasını kolaylaştırmak için, asgari düzeyde bir performans seviyesini garanti edebilecek bir QoS sağlamak gerekir. QoS, canlı etkinlik yayını gibi gecikmeye duyarlı uygulamalarda özellikle önemlidir ve bant genişliği kısıtlamaları nedeniyle elde edilmesi genellikle zordur. QoS’nin tanıtımı, ağ tarafsızlığı ilkesi için potansiyel bir zorluk da dahil olmak üzere TCP / IP’de değişiklik gerektirebilir.

Ağ teknolojilerinin sürekli evrimi ve burada vurgulanan zorluklar göz önüne alındığında, teknik topluluktaki kuruluşlar, gelişen teknik peyzajın gerçeklerine daha iyi uyan gelecek nesil İnternet protokolleri geliştirme olasılığını araştırmaya başlamışlardır. Örnek olarak, 2016 yılının başlarında, Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), ‘yeni nesil protokoller ve ağ mimarileri için gereklilikleri belirleme’ ile görevlendirilmiş bir çalışma grubu oluşturdu; grubun; adresleme, güvenlik ve kimlik doğrulama, NesNet’in gereklilikleri, video ve içerik dağıtım gereklilikleri ve e-ticaret gereklilikleri gibi meseleleri analiz etmeleri beklenmektedir.²⁸

www.igbook.info/protocols

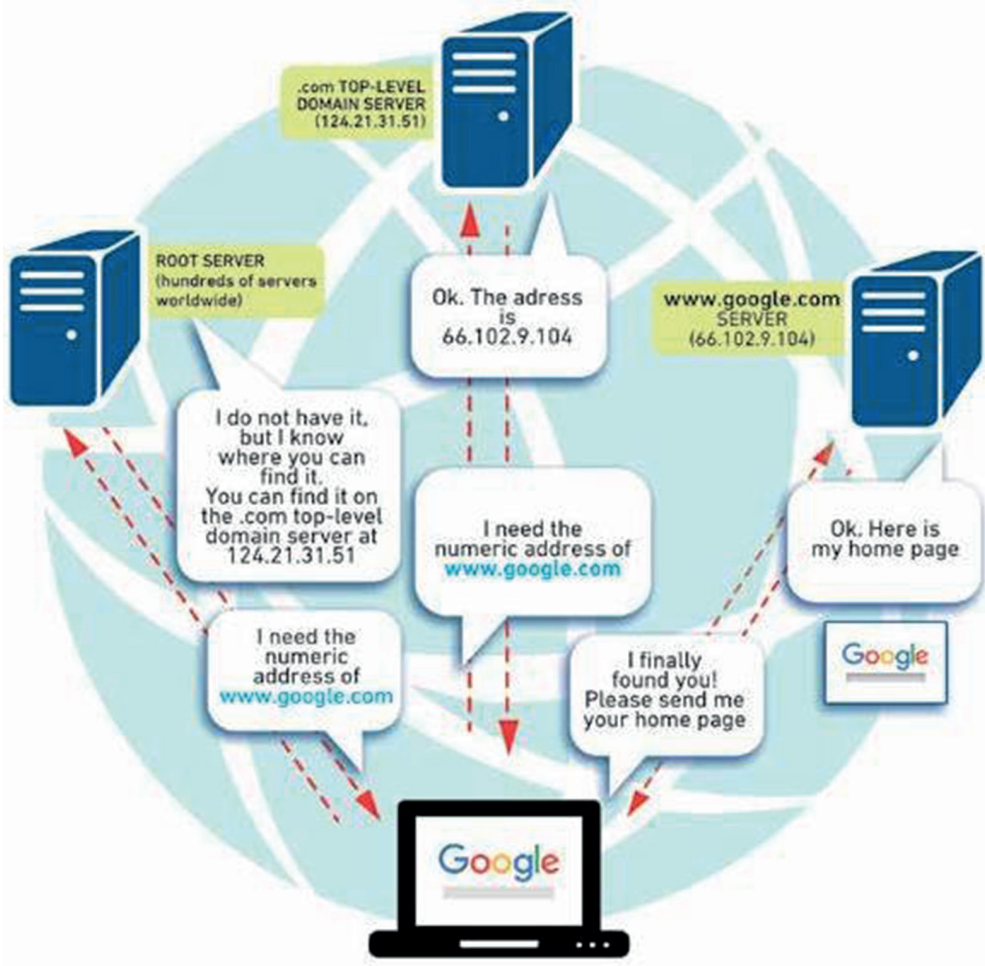
Alan Adı Sistemi

Mevcut durum

DNS, bireyler tarafından hatırlanması daha kolay olan (google.com gibi) İnternet alan adlarını belirli bir internet kaynağını belirlemek için bilgisayarlar ve diğer cihazlar tarafından kullanılan IP adreslerine çevirir (bu işlemin basitleştirilmiş bir şeması Şekil 8’de verilmiştir).

Altyapı açısından, DNS kök sunuculardan, üst düzey etki alanı (TLD) sunucularından ve dünyanın dört bir yanında bulunan çok sayıda DNS sunucusundan oluşmaktadır.²⁹

Bir TLD, İnternet’in hiyerarşik DNS’inde en üst seviyedir. DNS, iki ana üst düzey etki alanı türü içerir: **genel üst düzey etki alanları** ve **(ccTLD’ler gibi) ülke kodu üst düzey etki alanı**. gTLD’ler, com, .info, .net ve .org gibi geleneksel TLD’lerin yanı sıra, .pub, رازاب (çarşı), .rentals, .ngo veya □□ (oyun) gibi (2014 yılından itibaren piyasaya sürülen) nispeten yeni gTLD’leri içermektedir. Çoğu gTLD’nin açık bir kayıt politikası olmasına rağmen, alan adlarının ilgilenen herhangi bir kişi veya kuruluş tarafından kaydedilmesine izin verilmesine rağmen, belirli gruplara / sektörlerle / topluluklara sınırlı veya ayrılmış gTLD’ler de vardır. Örneğin, .aero sadece hava taşımacılığı endüstrisinde tescil için açıkken, .bank sadece yetkili bankacılık kuruluşları tarafından kullanılabilir. ccTLD’ler, belirli ülke veya topraklara atanmış belirten iki harfli TLD’dir (İngiltere için .uk, Çin için .cn ve Brezilya’dan .br gibi).



Şekil 8. DNS

Her gTLD ve ccTLD, asıl sorumluluğu ilgili TLD’de kayıtlı tüm etki alanı adlarıyla bir veritabanını korumak ve yönetmek olan bir **kayıt defteri** (**kayıt defteri operatörü** olarak da bilinir) tarafından yönetilir. Örneğin .com gTLD, VeriSign tarafından yönetilirken, .uk Nominet tarafından yönetilir. Etki alanı adlarının son kullanıcılar tarafından (**kayıt yapanlar** adı verilen) gerçek kaydı, **kayıt şirketleri** aracılığıyla yapılır. Çoğu durumda kayıt defteri ve kayıt defteri operatörlüğü işlevleri açıkça ayrılrsa da, istisnalar da vardır; örneğin ccTLD’ler için kayıt defteri operatörü kayıt görevini de gerçekleştirebilir.

ICANN, DNS’in genel koordinasyonunu:

- DNS kök bölgesindeki isimlerin tahsisini ve atanmasını koordine ederek,
- İkinci seviye alan adlarının gTLD’lerde kaydedilmesine ilişkin politikaların geliştirilmesi ve uygulanmasını koordine ederek,

- Operasyonun koordinasyonunu ve DNS kök adı sunucu sisteminin evrimini kolaylaştırarak sağlar.³⁰

ICANN konusundaki diğer tartışmalar için 9. Bölüme bakınız.

gTLD'ler için, ICANN (her gTLD'nin yönetimi için)³¹ kütükler ile ilgili anlaşmaları sonuçlandırır ve kütükleri kaydeden sicil memurlarını akredite eder.³² ICANN'ın nasıl yönetildiğiyle ilgili kuralları belirlemediği için ccTLD'ler özel bir statüye sahiptir. Bununla birlikte, özellikle iki taraf arasındaki ilişkiye ilişkin (hesap verebilirlik, mutabakat zaptı ve mektupların değişimi gibi) üst düzey ilkeler oluşturmak maksadıyla ICANN ile anlaşma yapmış olan birkaç ccTLD bulunmaktadır.

DNS'in operasyonel koordinasyonu, ICANN'ın bağlı kuruluşu PTI aracılığıyla gerçekleştirilmektedir.

Meseleler

Markalar

Alan adları ile ilgili hassas bir nokta, ticari markaların korunması ve ilgili uyumsuzluk çözüm mekanizmaları ile ilgilidir. İnternetin ilk günlerinde kullanılan alan adı tahsisinde ilk gelen ilk hizmeti alır ilkesi, genellikle daha sonra isimler üzerinde ticari marka haklarına sahip olan işletmelere yeniden satmak amacıyla, tescilli ticari markaları temsil eden alan adlarının kötü niyetle tescili uygulaması olarak, siber baskı olarak bilinen olguyu tetiklemiştir. ICANN ve Dünya Fikri Mülkiyet Teşkilatı (WIPO) tarafından geliştirilen [Tekdüzen Uyuşmazlık Çözüm Politikası](#) (UDRP), siber baskıları önemli ölçüde azaltan mekanizmalar sağlamaktadır.

Fikri mülkiyet konusundaki diğer tartışmalar için 4. Bölüme bakınız.

Mahremiyet ve verilerin korunması

Alan adları bağlamında diğer bir önemli unsur ise mahremiyet ve verilerin korunması ile ilgilidir. Halihazırda, kütükler tescil ettirenlerin verileri de dahil olmak üzere tescilli alan adları hakkında bilgi içeren WHOIS olarak bilinen veritabanlarını muhafaza etmektedir. WHOIS politikasının yeniden tasarlanmasını talep eden sivil hak savunucuları tarafından kamuya açık (isim, e-posta adresleri, posta adresleri gibi) bilgilere ilişkin endişeler dile getirilmektedir. Bu konuda tartışmalar son birkaç yıldır ICANN içinde de gerçekleştirilmiş ve WHOIS politikasını yeniden tasarlamayı amaçlayan bir süreç başlatılmıştır.

Yeni jenerik üst düzey alan adlarının yaratılması

2012 yılında, altı yıllık istişareler ve yeni bir politikanın geliştirilmesinden sonra, ICANN, DNS'yi o anda var olan 22 gTLD'nin ötesine açarak Yeni gTLD Programını başlatmıştır. Yeni

program kapsamında, dünyadaki herhangi bir kuruluş, [Yeni gTLD Başvuru Rehberi](#)'nde belirtilen bir dizi kritere uyduğu sürece, Latin dili olmayan betikler de dahil olmak üzere yeni bir gTLD kaydı çalıştırmak için başvurabilir. Yeni gTLD'lerin tanıtımı, programı alan adı pazarında rekabet ve tüketici seçimini artırma fırsatı olarak gören bazı paydaşlar tarafından coşkuyla karşılanmıştır. Bazıları da, özellikle ticari markaların artan sayıdaki gTLD bağlamında korunması ve ticari marka sahiplerinin siber baskıdan kaçınmak amacıyla potansiyel olarak çok sayıdaki gTLD'lerdeki alan adlarının kayıtlarını savunmacı şekilde üstlenmesi ihtiyacı ile ilgili olarak endişelerini dile getirmişlerdir. Yeni gTLD'lerin tanıtımı konusundaki tartışmalar devam etse de, program hala devam etmektedir; Eylül 2016'nın sonunda, (DNS'e tanıtılan) 1186 yeni gTLD'ye yetki verilmiştir.³³

Yeni gTLD'lerle ilgili tek endişe fikri mülkiyet konusu değildi. ICANN'nin Hükümet Danışma Komitesi'nde (GAC) temsil edilen hükümetler, son kullanıcıların korunmasını sağlayacak ve yeni gTLD'lere yetki verilmesi bağlamında uç kullanıcıları ve piyasadaki rekabeti koruyacak tedbirlerin uygulanması ihtiyacına dikkat çekmişlerdir. Örnek olarak, (.bank ve .pharm gibi) düzenlenmiş sektörleri temsil eden gTLD'ler söz konusu olduğunda, hükümetler, yalnızca ilgili sektörlerde faaliyet göstermek üzere uygun yetkilere sahip olan işletmelerin bu tür gTLD'lerde alan adlarını kaydetmelerini sağlayacak önlemler önermiştir.

Coğrafi adların ve göstergelerin korunması başka bir merak konusu olarak durmaktadır: Latin Amerika ülkeleri GAC içinde güçlü bir muhalefet oluşturduktan sonra ICANN, .amazon alan adı uzantısı için (çevrimiçi perakende satıcısı olan) Amazon'a yetki verme sürecinin durdurulmuştur. .wine veya .vin alan adı uzantılarına yetki verilmesi konusu, (bazı yargı kararlarında olduğu üzere) coğrafi işaretlerin yer aldığı şarap isimlerini temsil eden alan adlarının 'kötü niyetle kayıt altına alınması'nı engelleyecek önlemler alınmasını talep eden İsviçre ve Fransa gibi ülkelerle birlikte GAC içinde de yoğun şekilde tartışılmaktadır. ICANN .africa alan adı uzantısını uygulamaları Afrika Birliği ülkeleri (AU) ülkeleri tarafından uygun bulunan bir konsorsiyuma verdiğinde, bu karara özel bir şirket tarafından itiraz edilmiştir.

Ülke alan adlarının yönetimi

CcTLD'lerin yönetimi üç önemli konuyu içermektedir. Birincisi, (yeni bağımsız ülkeler, direniş hareketleri gibi) belirsiz veya çekişmeli uluslararası statüye sahip ülkeler ve kuruluşlarla ilgili tam olarak [hangi ülke kodlarının kaydedileceğine](#) ilişkin genellikle tartışmalı siyasi kararlarla ilgilidir. Geçmişte tartışmalı konulardan biri Filistin Otoritesi alan adının tahsis edilmesi konusuydu.³⁴ .ps üst düzey alan adı (TLD) uzantısının verilmesini gerekçelendirirken, IANA, İnternetin kurucu babalarından Jon Postel tarafından önerildiği gibi, ülke isimleri için ISO 3166 standardına uygun alan adlarının tahsis edilmesini ilke edinmiştir.

İkinci konu, [ccTLD'leri kimin yönetmesi gerektiği](#) ile ilgilidir. Halen, ccTLD'ler için birkaç kayıt modeli bulunmaktadır.³⁵ Bazı durumlarda, kayıt işlevleri (bir ulusal telekom düzenleme otoritesi, hükümet içindeki bir araştırma enstitüsü, bir devlet üniversitesi, vb gibi) bir kamu kuruluşu tarafından gerçekleştirilmektedir. Hükümetin, ccTLD'nin yönetimi için kuralları koyduğu, ancak gerçek yönetimi özel sektörün elinde bıraktığı ülkeler de vardır. Yine başka durumlarda, özel şirketler hükümetin dahli olmayan ccTLD'leri yönetmektedir. Ayrıca, yöne-

tim yapıları çeşitli paydaş gruplarının temsilcilerini içeren birkaç çok paydaşlı ccTLD kütüğü de bulunmaktadır.³⁶

İnternetin ilk günlerinde, hükümetler ccTLD'lerle çok fazla ilgilenmiyor gibi görünüyorsa da, bazı hükümetler ulusal kaynaklar olarak kabul ettikleri ülke alanları üzerinde kontrol sahibi olmaya çalışırken, yıllar içinde işler değişmiştir. Ulusal hükümetler çok çeşitli politika yaklaşımları tercih etmektedir.³⁷ Her ülkede ccTLD'yi yöneten yeni bir (yetkili) kuruma (yeniden yetkilendirme ile) geçiş, ancak ülke içindeki ilgili paydaşların herhangi birinden bir karşı çıkış yoksa ICANN tarafından onaylanmaktadır.

Üçüncü sorun, gTLD'lerin aksine, **ICANN'ın ccTLD'leri kimin yönetmesi gerektiği ve bunların nasıl yönetilmesi gerektiği konusunda hiçbir kural getirmediği** gerçeğiyle ilgilidir. ICANN sadece, ccTLD'lerin onu yönetme konusunda teknik olarak yetkin olmasını ve bunu yapmak için yerel topluluğun desteğine sahip olmasını sağlamayı amaçlayan bazı üst düzey kurallara dayanarak ccTLD'lerin yetkilendirilmesi veya yeniden yetkilendirilmesi ile ilgilenmektedir.³⁸

2005 yılında, ICANN'ın Hükümet Tavsiye Komisyonu (GAC), hükümetler, ccTLD'ler ve ICANN arasındaki ilişkileri düzenlemek için **ülke kodu üst düzey alanlarının delegasyonu ve idaresi için bir dizi Ülke ve Kılavuz**³⁹ ortaya koymuştur. Yasal olarak bağlayıcı bir statüye sahip olmayan bu belgede ana hatları çizilen temel ilkelerden birisi, sorunun küresel etkiye sahip olduğu ve uluslararası çerçevede çözülmesine ihtiyaç olduğu gösterilmediği sürece, 'ccTLD politikasının yerel olarak ortaya koyulması gerektiğini' ifade eden yerindenlik ilkesidir.

Daha önce belirtildiği gibi, ICANN ile bir tür anlaşmaya varılan ve aralarındaki ilişkiyi düzenlemek için üst düzey ilkeler belirleyen (Brezilya, Şili, Hollanda, İsveç ve Birleşik Krallık'takiler gibi) birkaç ccTLD kütüğü vardır. Ayrıca, (Uluslararası Alan Adlarının (IDN'ler) ortaya konulması gibi) ccTLD ile ilgili sınırlı konularda küresel politikaları geliştiren ve ICANN Kuruluna tavsiye eden ICANN bünyesinde Ülke Kodlarını Destekleme Teşkilatında (ccNSO) temsil edilen pek çok küttük de bulunmaktadır. Bununla birlikte, aynı zamanda, bazı ccTLD kütükleri ICANN sisteminin bir parçası olma konusundaki isteksizlik göstermiştir (Eylül 2016'da, o sırada 240'dan fazla ccTLD varken ccNSO sadece 161 üyeye sahipti).

Ülke etki alanı operatörleri bölgesel düzeyde organize edilmektedir: Avrupa - Avrupa Ulusal Üst Düzey Etki Alanı Kütük Kurulları (CENTR), Afrika - Afrika Üst Düzey Etki Alanları Örgütü (AFTLD), Asya - Asya Pasifik Üst Düzey Etki Alanı Derneği (APTLD), ve Latin Amerika ve Karayipler - Latin Amerika ve Karayipler ccTLD Organizasyonu (LACTLD) gibi.

Uluslararası alan adları

İnternet başlangıçta ağırlıklı olarak İngilizce bir dilinin aracı olduğu bir ortamdı. Hızlı büyüme sayesinde, artan sayıda İngilizce konuşamayan kullanıcıyla küresel bir iletişim ortamı haline geldi. Uzun süredir İnternet altyapısındaki çok dilli özelliklerin eksikliği internetin gelecekteki gelişiminin önündeki temel sınırlamalardan birisiydi.

IDNs are also part of ICANN's New gTLD Program, allowing for the registration of new gTLDs in scripts other than Latin; for example, .сайт (website) and .онлайн (online) are among the new TLDs available to the public.

Mayıs 2010'da, uzun bir test süresinin ve politik belirsizliklerin ardından, ICANN, Çince, Arapça ve Kiril gibi çok çeşitli komut dosyalarında TLD'leri onaylamaya başladı. IDN'ler birçok ülke ve bölgede Latin ccTLD'lerine eşdeğer olarak ortaya konulmuştur. Örneğin, Çin'de .cn'ye ek olarak 中国 tanıtılırken, Rusya'da .ru'ya ek olarak ayrıca рф ortaya konulmuştur. IDN'ler ayrıca, ICANN'ın Yeni gTLD Programının bir parçası olup, yeni gTLD'lerin Latin dilleri dışındaki komut dosyalarına kaydedilmesini sağlar; örneğin, .сайт (web sitesi) ve .онлайн (çevrimiçi) halka sunulan yeni TLD'ler arasındadır.

IDN'lerin tanıtımı, İnternet yönetim rejiminin ana başarılarından biri olarak kabul edilir. Bununla birlikte, özellikle tüm e-posta adreslerinin herhangi bir komut dosyasında kullanılmasını sağlamakla ilgili diğer teknik engeller var: e-posta adreslerinde TLD zaten bir IDN olabilirken, e-postanın ilk kısmı (yani, @ işaretinden önceki olanın hala Latin alfabesinde yazılması gerekir. IDN'lerin arama motorları tarafından tanınması da ele alınması gereken bir konudur. Özel ICANN gruplarının ilgilendiği bu teknik sorunun yanı sıra, IDN'lerin yaygın olarak kullanılmasını sağlamak için hala bir zorluk var; bu, Latin olmayan bir senaryo kullanan ülkelerde bu seçenek hakkında farkındalığın artırılmasını gerektirir. Hizmetlerin ve içeriğin oluşturulması da yüksek önceliğe sahip olmalıdır.

www.igbook.info/dns

Kök bölgesi ve kök sunucular

NS hiyerarşik yapısının en tepesinde kök sunucular İnternet yönetişimi konularındaki politik ve akademik tartışmalarda oldukça fazla dikkat çekmektedir.

Mevcut durum

DNS'nin işlevi ve sağlamlığı, kök sunucular hiç devre dışı bırakılırsa İnternet'in çökeceği konusu analiz edilerek gösterilebilir.

Kök bölge, DNS teknik yapısındaki en yüksek seviyedir. Kök bölge dosyası, DNS'deki tüm TLD'lerin (hem gTLD'ler hem de ccTLD'lerin) adlarının ve IP adreslerinin listesini içerir.⁴⁰ Kök bölgesinin yönetimi, ICANN'ın IANA işlevlerinin işleyişindeki bağlı kuruluşu PTI tarafından gerçekleştirilmektedir. Bu rolü yerine getirirken, PTI, TLD operatörlerini tayin eder ve teknik ve idari detayları ile birlikte bir veritabanı tutar. Kök bölge dosyasının bakımı (güncelleme) VeriSign tarafından gerçekleştirilir. Başlangıçta VeriSign ile ABD hükümeti arasındaki işbirliğine dayalı bir anlaşma temelinde gerçekleştirilen bu kök bölge koruma işlevi, IANA yönetimi geçişi bağlamında, ICANN ile VeriSign arasındaki bir anlaşmayla değiştirilmiştir.

DNS kök bölgesi, kök bölge dosyasının kamuya açık kopyasını tutan yetkili sunucular olarak da bilinen kök sunucular tarafından sunulur. Toplam kök sunucu sayısının 13 olduğu yanlışlığı vardır. Gerçek, dünyanın çeşitli yerlerine dağılmış yüzlerce kök sunucusunun var olduğudur.⁴¹ 13 sayısı, DNS tasarımıdaki teknik bir sınırlamaya bağlı olarak 13 farklı ana bilgisayar adından gelir.⁴² Altısı akademik veya kamu kurumu, üçü ticari şirket, üçü hükümet kuruluşu olan

oniki kurum bu birincil aşamaları yönetir ve aynı aşamalar içerisinde yer alan tüm kök sunucuların kök bölge dosyasının güncellenmiş kopyasına sahip olmalarını güvence altına alır.

13 ana bilgisayar adından biri çıktığında, kalan 12 işlevi çalışmaya devam eder. 13'ünün tümü aynı anda çökse bile, (kök sunucuların ana işlevi olan) alan adlarının IP adreslerine dönüşmesi işlevi, İnternet üzerinden hiyerarşik olarak dağıtılan diğer alan adı sunucularında devam eder.

Kök sunucuların sistemi, dünya genelinde kök sunucuların çoğalmasını yapan Anycast programı⁴³ ile büyük ölçüde güçlendirilmiştir. Bu, DNS'nin sağlamlığının artırılması ve İnternet adreslerinin daha hızlı çözülmesi (Anycast programı ile, çözümleyen sunucular son kullanıcılara daha yakın olması) gibi birçok avantaj sağlar.

Bu nedenle, yüzlerce alan adı sunucusu, kök bölge dosyasının kopyalarını içermekte ve İnternet'in hemen ve feci bir çöküşü gerçekleşemez. Ciddi fonksiyonel sonuçların farkına varılması biraz zaman alacaktır, bu süre zarfında orijinal sunucuları yeniden etkinleştirmek veya yenilerini oluşturmak mümkün olacaktır.

Daha önce belirtildiği gibi, kök bölge dosyası VeriSign tarafından korunur ve güncellenir. Örneğin, ICANN tarafından yeni bir gTLD onaylandığında, bu bilgiler (yeni gTLD'yi köke getirerek) kök bölgede gerekli değişiklikleri yapan ve revize edilmiş kök bölge dosyasını kök ismi sunucularına dağıtan VeriSign'a iletilir.

Meseleler

Alternatif kök sunucuları – fizibilite ve riskler

Biri, ICANN'ın neden TLD listesini ve IP adreslerine çözüm yollarını dikte etme hakkına sahip olduğunu sorabilir - mevcut DNS sistemine alternatif bir seçenek olamaz mı? ICANN - IANA işlev operatörü olarak çalışan PTI üzerinden - alan adlarını IP adreslerine çözümlemek için kişisel İnternet kullanıcılarının çoğu tarafından alan adlarını IP adreslerine dönüştürmede kullanılan resmi DNS kökünü çalıştırır ve yönetirken, bazı kuruluşlar etkin alternatif DNS kökleri (Alternatif Kökleri) kullanmaktadır. Bu tür kuruluşlar genellikle ICANN TLD listesinde oldukça farklı olan kendi TLD izinlerini sunsa da böyle bir hizmeti kullanmak isteyen son kullanıcıların, evrensel kökünden alternatif köke sapmak için ağ ayarlarını yeniden yapılandırmaları gerekir. İlk alternatif köklerden biri, 1995 yılında kurulan ve 1998'de ICANN oluşumuna kadar işlevselliğini sürdüren AlterNIC'dir.

Alternatif bir DNS oluşturmak için başka birkaç deneme, Open NIC, New.net ve Name.space tarafından yapılmıştır. İnternet kullanıcılarının sadece yüzde birkaçını oluşturan bu denemelerin çoğu başarısız olmuştur.

Şu anda, Google DNS, Open DNS, Advantage DNS ve ScrubIT dahil olmak üzere birkaç alternatif DNS sunucusu kurulmuş ve çalışmaktadır.⁴⁴

Nispeten yeni ve daha iddialı bir proje olan 2015 yılında başlatılan Yeti DNS Projesi, 'DNS kök adı hizmetinin sınırlarını keşfetmek için paralel deneysel canlı bir IPv6DNS kök sistemi' kurmayı planlamaktadır.⁴⁵

Alternatif bir kök isim sunucusu sistemi oluşturmak teknik olarak basittir. Asıl soru, alternatif bir sistemin kaç takipçiye sahip olacağı veya daha kesin olarak, alanı adlarını çözümlmek için İnternet'teki kaç bilgisayarın alternatif sunuculara yöneleceğidir. Kullanıcılar olmadan, alternatif bir DNS yetersiz olacaktır.

Kavramsal tartışma: alternative kök sunucu sistemine karşı tek sunucu sistemi

Uzun süredir, tek kök isim sunucusu sistemi ilkesi dokunulmaması veya hatta tartışılmaması gereken ana İnternet mantralarından biri olarak kabul edildi. Tek sisteme alternatifler hakkında tartışma yapılmasını önlemek için çeşitli argümanlar ileri sürülmüştür. Bir argüman mevcut sistemin DNS'nin bazı hükümetler tarafından sansür için kullanılma riskini önlediği yönündedir. Bununla birlikte, DNS politikasındaki değişikliklere karşı sansür argümanı işlevsel olarak temellerini kaybetmektedir. Hükümetlerin sansür sağlamak için DNS sistemi veya kök bölge dosyası üzerinde kontrole ihtiyaçları yoktur. Hükümetler web trafiğinin filtrelenmesine dayanan daha etkili araçlara müracaat edebilirler.

Daha sağlam bir argüman, herhangi bir alternatif kök sisteminin bölünmeye ve hatta belki de İnternet'in nihai parçalanmasına yol açabileceğidir. Tüm kök sistemlerin aynı IP numaraları sistemini kullanmasına rağmen, farklı adlandırma yaklaşımları ve çözümler teknikleri kullanılmaktadır. Birkaç kök sistemi aynı alan adına sahip olması mümkündür, ancak her biri farklı bir IP adresine dönüşmektedir. Bununla birlikte, alternatif DNS köklerinin çoğu, ICANN'ın DNS kökü ile veya kendi aralarında ortaklaşa çalışmadıkları için, alternative kökler kamusal değil de tamamen özel amaçlı kullanılmadıkça, bir arada bulunmaları, bir TLD'yi bir IP adresine dönüştürmenin tek bir yolu olmasını sağlayan evrensel dönüştürme ilkesini ihlal edecektir. DNS açısından bakıldığında da, İnternet'in bazı bölümlerinin diğer bölümlere ulaşmasını engelleyecektir. İnternetin parçalanması, birleşik bir küresel iletişim sistemi olan İnternet'in temel işlevlerinden birisini tehlikeye atabilir. Bu tehlike ne kadar gerçekçi olabilir.⁴⁶

www.igbook.info/root

Ağ tarafsızlığı

İnternet'in başarısı, ağ tarafsızlık ilkesine dayanan tasarımında yatmaktadır. Başlangıçtan itibaren, tüm İnternet içeriğindeki veri akışı, ister yeni başlayanlardan isterse büyük şirketlerden gelsin, ayırım gözetilmeksizin ele alınmıştır. Yeni şirketler ve yenilikçiler İnternette yenilik yapmak için izin veya pazar gücüne ihtiyaç duymamışlardır. Yeni dijital hizmetlerin kullanımı ve gelişmesindeki büyüme, özellikle de yüksek kaliteli video akışı gibi yüksek bant genişliğini tüketenlerin büyümesiyle, (telekom şirketleri ve İSS'ler gibi) bazı İnternet operatörleri ağı daha fazla yatırım yapmak için gereken fonları artırma ihtiyacını ileri sürerek bu tür bir yaklaşımın haklı çıkarmak için işletme ihtiyaçları ve planlarına dayanarak kendi servisleri veya kendi iş ortaklarının servisleri gibi belirli internet trafiğine öncelik vermeye başlamıştır. Ağ tarafsızlığının savunucuları, bunun, bilgiye ve çevrimiçi özgürlüklere açık erişimi kısıtlayabileceğini ve çevrimiçi yenilikleri boğabileceğini ileri sürerek bu tür planlara karşı şiddetle direnmektedir.

İnternetin başarısı için ağ tarafsızlığın önemi çok büyüktür. Ağ tarafsızlık ilkelerini koruma konusundaki tartışmalar, ABD Başkanı Obama'dan insan hakları aktivistlerine kadar çok çeşitli aktörleri içine çekmiştir. Ağ tarafsızlığın nasıl ele alındığı, İnternet'in gelecekteki gelişimini etkileyebilir.

Mevcut Durum

Birileri ağ tarafsızlığı ve ağ trafiği yönetimi arasında bir ayrım yapmak zorundadır. İnternete çevirmeli ağ modemi ile bağlanmanın ilk günlerinden beri, ağ trafiği yönetimi, mevcut bant genişliği ve kullanıcıların bant genişliği ihtiyaçları arasındaki boşlukla uğraşmak için kullanılmıştır. Bu zorluğun üstesinden gelmek ve kaliteli hizmet sunmak için, genellikle taşıyıcılar olarak da adlandırılan (telekom şirketleri ve İSS'ler gibi) İnternet operatörleri belirli trafiğe öncelik vermek için çeşitli trafik yönetimi tekniklerini kullandılar. Örneğin, VoIP servisleri üzerinden sesli görüşme yapan İnternet trafiği (örneğin, Skype), basit bir e-posta taşıyan trafiğe göre önceliğe sahip olmalıdır: Skype'da sesli sohbetteki gecikmeleri duyabildiğimiz halde, e-posta alış-verişinde küçük gecikmeler görmeziz.

Trafik yönetimine duyulan ihtiyaç, özellikle yüksek bant genişliği taleplerinin artması nedeniyle bugün için çok önemlidir: Giderek daha fazla sayıda kullanıcı düzenli olarak (Skype, Google Hangout, telekonferans gibi) sesli ve görüntülü İnternet aramalarını kullanır, çevrimiçi oyunları oynar veya (Hulu veya Netflix gibi hizmetler gibi) TV şovları ve filmleri HD kalitesinde izler hale gelmiştir. Trafik yönetimi, bir yandan mobil cihazların kullanımının artması ve bir yandan da kablosuz spektrumun teknik sınırları nedeniyle kablosuz iletişim açısından önemlidir.⁴⁷ Trafik yönetimi, kaliteli hizmet sunmak, tıkanıklığı önlemek ve gecikmeyi ve sarsıntıyı ortadan kaldırmak için İnternet trafiğini en uygun şekilde yönlendirmek için giderek daha karmaşık hale gelmektedir.

Ağ tarafsızlık ilkesinin yorumlanmasındaki ilk fikir ayrılığı, herhangi bir trafik yönetimine izin verilip verilmeyeceğine odaklanmıştır. Ağ tarafsızlık uzmanları, "tüm bitlerin eşit yaratıldığını" ve tüm İnternet trafiğinin eşit şekilde ele alınması gerektiğini savunmuştur. Telekom ve İSS'ler bu görüşe, İnternet servislerine eşit erişime sahip olması gerekenin kullanıcılar olduğunu ve bu olacaksa İnternet trafiğinin eşit şekilde ele alınamayacağını savunmuştur. Örneğin, hem video hem de e-posta trafiği eşit olarak ele alınırsa, kullanıcılar iyi bir video akışı alımına sahip olmayacak, ancak bir e-posta alırken birkaç saniye gecikmeyi farketmeyeceklerdir. Ağ tarafsızlığı uzmanları bile bu mantığı sorgulamayı bırakmıştır.

Meseleler

Ağ tarafsızlığı tartışmasında, uygun trafik yönetimine duyulan ihtiyaç çevresinde ortaya çıkan bir fikir birliği vardır. Asıl soru neyin uygun olduğunun nasıl belirleneceğidir. Teknik kaygıların yanı sıra, trafik yönetimi ve ağ tarafsızlığı tartışmasının özellikle sıcak olduğu iki alan bulunmaktadır: konunun ekonomik yönü ve insan hakları sorunları.

Ekonomik yön

Geçtiğimiz on- yirmi yıl boyunca, telekom ve ISS'ler gibi birçok önemli ağ operatörü iş modellerini değiştirmeye başlamıştır: hane halklarına ve işletmelere İnternet erişimi sağlamanın yanı sıra, talep üzerine video, müzik veya video indirmek gibi kendi VoIP veya IPTV hizmetlerini sunmaya başlamışlardır. Artık yalnızca daha ucuz, daha hızlı ve daha kaliteli bağlantılar sağlamak için rakipleriyle değil, aynı zamanda Google, Facebook, Netflix ve Skype gibi içerik ve servis sağlayıcıları gibi OTT hizmet sağlayıcıları ile de rekabet etmektedirler.

Trafik yönetimi, işletme odaklı tercihlere göre paketleri önceliklendirerek hizmet ve içerik sunumunda rekabet ederken önemli bir araç olabilir. Örneğin, bir operatör (müşterilere sunduğu IP telefon veya İnternet televizyonu gibi) kendi veri paketlerine öncelik verirken, (Skype veya Google Voice gibi) rakip bir şirketten gelen veri paketlerinin akışı son kullanıcılar için ağ üzerinden yavaşlatmaya veya tamamen yasaklamaya karar verebilir.⁴⁸

Aynı zamanda, operatörler daha çok OTT servisleri tarafından istenen daha fazla bant genişliği talebinin temel altyapıya daha fazla yatırım yapılması gerektiğini ileri sürmektedir. OTT servis sağlayıcıları genişletilmiş talebe en fazla katkıda bulunanlar ve gelişmiş altyapıdan en fazla yararlananlar oldukları için, operatörler OTT'nin de dahil olacağı sağlayıcıların finansmana katkıda bulunabileceği çok katmanlı bir ağ politikası modelinin OTT hizmetleri için gereken hizmet kalitesini garanti edeceğini ileri sürmektedir. Bu gibi durumlar bir kez daha, trafik yönetiminin teknik nedenlerden çok ekonomik nedenlerle kullanıldığını göstermektedir.

Gelirleri artırmak için telekom endüstrisi yeni iş modelleri veya düzenlemeler tasarlamaya devam etmektedir.

Bir yandan, mobil telekom sağlayıcıları tarafından müşterilere sunulan **katma değer vergisi sıfır dereceli hizmetler**, belirli uygulamaların veya servislerin sınırsız (ücretsiz) kullanımına izin vermektedir. Bazı durumlarda, bu tür uygulamalara veya hizmetlere erişim bir abonenin veri eşliğine sayılmazken, diğer düzenlemelerde, kullanıcıların bir veri planı olmadan da erişimine izin verilir. Tüm dünyada giderek daha fazla yer almasına rağmen, sıfır katma değertartışmalı bir konu haline gelmiştir. Bu hizmetler mobil veri servislerine erişimin ortalama gelirden daha pahalı olduğu gelişmekte olan ve en az gelişmiş ülkelerde bazıları tarafından özellikle önemli görülmektedir. Sıfır katma değer lehine olan temel argümanlardan biri, (bir veri planının bir parçası olarak teklif edildiğinde) çevrimiçi bilgilere erişim maliyetini düşürdüğü ve (bedava erişim sağladığında) parası olmayan kullanıcılara (bazı) çevrimiçi bilgilere erişim sağlamasıdır. Bunu destekleyenler, bazı bilgilere erişimin, hiçbir erişimin olmamasının tercih edildiğini; Ayrıca olarak, kullanıcılara belirli türden uygulamalara ücretsiz erişim sağlamanın genel İnternet erişimi için talep yaratabileceği ve böylece işletmecilerin altyapı inşa etmek ve dağıtmak için yatırım yapmalarını teşvik edeceği ileri sürülmektedir.

Öte yandan, bu argümanın karşıtları sıfır katma değer düşüncesinin başka hizmetlere göre bazı hizmetlere öncelik verdiğini ve dolayısıyla piyasa rekabeti ve inovasyona zarar vererek ağ tarafsızlığı ilkesine karşı olduğunu savunmaktadır. Bazıları ayrıca, sıfır katma değer düşüncesinin kullanıcıların insan haklarına etkileri konusundaki endişelerini dile getirmektedir. e ilişkin endişelerini de dile getirmiş, bu tür hizmetlerin bir kullanıcının (daha geniş ifade özgürlüğü

hakkının bir parçası olarak görülen) bilgi alma hakkıyla ihtilafa düşebileceğini ifade etmişlerdir.

Sıfır katma değer konusundaki tartışmalar, 2014 yılında Free Basics hizmetinin başlatılmasının ardından daha yoğun hale gelmiştir. Facebook tarafından, gelişmekte olan ve daha az gelişmiş birkaç ülke denemesinde sunulan hizmet, mobil iletişim kullanıcılarının (Facebook'a ek olarak) Wikipedia ve AccuWeather gibi uygulamalara ücretsiz erişmesine imkan vermektedir. Bu tartışmalar, hizmetin daha önce tanıtıldığı (Hindistan ve Mısır gibi) bazı ülkelerde hizmetin askıya alınmasına yol açmıştır.

Aynı zamanda, sıfır katma değerli hizmetlerin yanı sıra, telekomlar gelecekte sunulabilecek yüksek kalite ve özel iyileştirme gerektiren, yüksek bant genişliği gerektiren HD video akışı veya ve e-çözümler gibi 'özel servisler'den de bahsetmektedir.

Çok katmanlı bir İnternet önerileri, yıllardır ağ tarafsızlığı konusundaki tartışmaların merkezinde yer almaktadır. Bu tür bir öneri, 2010 yılında Verizon ve Google tarafından öne sürülen ve işletmeler açısından İnternet'in 'ilave çevrimiçi hizmetler' biçiminde önerildiği [Açık İnternet Yasal Çerçevesi Önerisi](#)⁴⁹ idi. Bu tür modellerin savunucuları bunun kullanıcılar için daha fazla hizmet seçeneği getireceğini ve altyapıya yatırım yapılmasını teşvik edeceğini ileri sürerken; muhalifleri bunun hem ekonomik hem de ticari açıdan (kablolu spektrum ve kablolar gibi) aynı 'hatları' etkili şekilde kullanılarak en iyi çaba ağına zarar vereceğinden korkmaktadır.

Bu arada, pazar İnternet'in çalışma biçiminde değişiklikler getirdi: geçiş maliyetlerini ve zamanını azaltmak için, içerik sağlayıcılar İçerik Dağıtım Ağları (CDN'ler) kurarak kullanıcılara daha fazla yaklaşıyor - bölgesel İnternet Borsasına yakın yerleştirilmiş sunucuları ön belleğe alıyor Nokta (IXP) hub'ları veya büyük bölgesel telekom içinde. Bu, ağ performansını ve maliyetlerini iyileştirdi. Başlangıçta bir CDN sağlayabilen (ve ihtiyaç duyan) büyük içerik sağlayıcılar olmasına rağmen, veri merkezleri ve bulut sağlayıcılar için bir pazarın ortaya çıkması, bir bulutun bulunmasını sağlayan bir CDN'nin açık pazarda kullanılabilmesini sağlar. CDN servislerini kiralamak için dünyanın her yerindeki kullanıcılara hizmet etmesi gereken servis.

Çok katmanlı İnternet

İnternet trafiği halihazırda "en iyi gayret" yaklaşımı ile sunulmaktadır: bu, belirli bir QoS, etkin hız veya veri paketlerinin teslim süresi konusunda hiçbir garanti vermemektedir. Tam tersine, kullanıcılar mevcut bant genişliğini paylaşmakta ve o sırada trafik yüküne bağlı olarak değişen bit sayıları (hız) elde etmektedir.⁵⁰ Trafik yönetimi bu nedenle son kullanıcılar için etkin hizmet kalitesinde önemli bir rol oynamaktadır.

Çok katmanlı İnternet kavramı, İnternet'e, yani en iyi gayretin ötesinde garantili bir QoS içeren özel hizmetler sunmaya yönelik bir "iş katmanı" anlamına gelir. Bunu ileri sürenler, iş katmanının en iyi çabaya dayanacak olan ekonomik katmana (şu anda bildiğimiz İnternet) paralel olarak devam edeceğini ifade etmektedirler. OTT servis sağlayıcıları, hizmetlerini işletme katmanı yoluyla belirli maliyetle veya en iyi çaba ağıyla bir maliyet olmadan kullanma seçeneğine sahip olacaklardır.

İnsan hakları mevzuları

Ağ tarafsızlık ilkelerinin ihlal edilmesinin sonuçları sadece ekonomik değildir. İnternet, bilgiye erişim, ifade özgürlüğü, sağlık ve eğitim de dahil olmak üzere temel insan haklarıyla bağlantılı modern toplumun ana direklerinden biri haline gelmiştir. Açık İnterneti tehlikeye sokmak temel hakları etkileyebilir.

Kullanıcılar mı müşteriler mi?

Net tarafsızlığı tartışması dil bilimsel tartışmaları tetiklemektedir. Net tarafsızlığın savunucuları internet 'kullanıcılarına' odaklanırken, çoğunlukla ticari oyuncular olan diğerleri onları 'müşteriler' olarak tanımlamaktadır. İnternet kullanıcıları sadece müşteriden daha fazlasıdır; 'kullanıcı' terimi, onların sosyal ağ çalışmaları, blog ve diğer araçlar aracılığıyla İnternet'in gelişimine aktif katılımı ve İnternet'in geleceğine karar vermede önemli rol oynadıklarını ifade eder. İnternet hizmetleri müşterileri, diğer müşteriler gibi, sunulan hizmetleri satın alıp almayacağınıza da karar verebilir. İnternetteki durumları, ISP ve müşteri korumaya ilişkin kurallar ile yapılan bir sözleşmeye dayanmaktadır. Bunun ötesinde, müşterilerin İnternet'in nasıl çalıştırıldığına karar vermede herhangi bir rolü olmadığı varsayılmaktadır.

Buna ek olarak, ağ trafiğini hizmet veya içerik üzerinden çıkış noktasına veya varış noktasına göre yönetmek yetkililere ülkenin politik, ideolojik, dini, kültürel veya kültürel durumuyla ilgili sakıncalı ve hassas içerikli İnternet trafiğini filtreleme fırsatı verebilir. Bu durum internet trafiği yönetimi yoluyla siyasal sansür için olanakların yolunu açar.

Asıl oyuncular kimlerdir ve neyi iddia etmektedirler?

Ana oyuncuların ağ tarafsızlığı tartışmasındaki pozisyonu sürekli bir dalgalanma halindedir. Ağ tarafsızlığının temel savunucularından bazıları, tüketici hakları savunucuları, çevrimiçi şirketler, bazı teknoloji şirketleri, Google, Yahoo!, Vonage, eBay, Amazon, EarthLink ve Microsoft gibi birçok büyük İnternet uygulama şirketidir.

Ağ tarafsızlığın karşıtları arasında başlıca telekom şirketleri, ISS'ler, ağ ekipmanı ve donanımı üreticileri ile video ve multimedya materyalleri üreticileri yer almaktadır. Bunların ağ trafiği yönetimine ilişkin düzenlemelere ilişkin karşı argümanları, tüketicilerin istediklerini sunma ihtiyacından başlayarak pazar merkezlidir. Telekom operatörlerinin ağ tarafsızlığıyla ilgili herhangi bir düzenlemeye karşı çıkma eğiliminin aksine, Avrupa Telekomünikasyon Ağı Operatörleri (ETNO) WCIT'-12'ye ağ tarafsızlığı koruyan daha fazla ulusal düzenlemenin önlenmesi için uluslararası düzenleme teklif etmiştir. Ancak Verizon gibi ABD'li şirketler ETNO'nun bu girişimine karşı çıkmıştır.⁵¹

Ağ tarafsızlığı tartışmalarında öne çıkan dört temel argüman Tablo 1'de özetlenmektedir.

Table 1. Ağ tarafsızlığı tartışmalarındaki dört temel argüman

Argüman	Ağ bağımsızlığı savunucuları	Ağ bağımsızlığı karşıtları
Geçmiş/gelecek argümanı	İnternetin açık mimarisi sayesinde yeni İnternet şirketleri gelişti ve son kullanıcılar net tarafsızlığı sayesinde yeniliklerden ve hizmet çeşitliliğinden yararlanmaktadır. Net tarafsızlığı, İnternetin şimdiye kadar hızlı ve yenilikçi bir şekilde gelişmesini sağlayan İnternet mimarisini koruyacaktır.	Trafik yönetimi kaçınılmazdır ve tarafsızlık hiç yaşanmamıştır. Ayrıca, VPN'ler (sanal özel ağlar) gibi zaten nötr olmayan kiralanan hizmetler vardır. Ağ tarafsızlığı kısıtlamaları olmadan, İnternet şirketleri müşterileri için garantili QoS ile yeni hizmetler geliştirebilirler.
Ekonomik argüman	Net tarafsızlığı olmadan, İnternet kablolu TV'ye benzecektir: bir avuç büyük şirket, içeriğin erişimini ve dağıtımını kontrol ederek kullanıcıların ne göreceğine ve onlara ne kadar mal olacağına karar verecektir. Yeni başlayanlar ve özellikle gelişmekte olan ülkelerdeki küçük işletmeler gelişme şansına sahip olmayacaktır. OTT servis sağlayıcıları, internet bağlantıları için telekomünikasyon şirketlerine zaten çok para ödüyorlar ve önbellekleme sunucuları gibi altyapıya yatırım yapıyorlar.	İçerik ve hizmet sağlayıcılarla yapılan ticari anlaşmalarda ağ tarafsızlığı kısıtlamaları olmadan, telekom operatörleri, altyapıya daha iyi yatırım yapmalarını daha fazla ilgilendirmelerini sağlayacak fonlar yaratabilecektir. Daha iyi bir altyapı, müşterilerin ihtiyaçlarına daha uygun hale getirilmiş ve herkese daha fazla gelir getiren yeni hizmetleri ve yenilikleri teşvik edecektir. OTT servis sağlayıcıları ayrıca ağ tarafsızlığı hükümleriyle kısıtlanmadığı takdirde, operatörler tarafından sağlanan QoS ile mümkün olan yenilikçi servisler de değer bulacaklardır.
Etik argüman	İnternet, birçok gönüllünün on yıllardır yaptığı gelişmelerin sonucudur. Teknik protokollerden içeriğe kadar her şeye zaman ve yaratıcılık kazandırdılar. İnternet bir işten daha fazlasıdır; insanlığın küresel mirası haline gelmiştir. İnterneti kısıtlı iş modellerinde net tarafsızlığını ihlal ederek kilitleyen ve birçoğunun yaratıcılığını bir kaçının karına dönüştüren yalnızca birkaç şirket tarafından toplanan bu kadar büyük bir zaman ve yaratıcılık yatırımına sahip olunması haklı değildir.	Net tarafsızlığı etik olarak sorgulanabilir çünkü operatörlerin yeni hizmetleri desteklemek için İnternet altyapısını korumaya ve genişletmeye yatırım yapmaları gerekirken, en büyük faydayı Google'ın, Facebook ve Amazon gibi İnternet 'içeriği' şirketleri sağlamaktadır.
Düzenleme argümanı	Kamunun menfaatini korumak için hükümet tarafından net tarafsızlığı sağlanmalıdır. Her türlü kendi kendine düzenleme, operatörlerin net tarafsızlığı ilkesini ihlal etmesine açık bırakacaktır. Büyük küresel telekom internet altyapısının çekirdeğinde olduğundan, açık pazar yeterli bir mekanizma değildir. Seçme olasılığı olsa bile, kullanıcılar teknik ve yasal okuryazarlığa ve mevcut çeşitli seçeneklerin sonuçlarının farkındalığına ihtiyaç duyduğundan bu her zaman gerçekleşmez.	İnternet çok hafif ya da hiç düzenleme olmadığı için gelişti. Ağır hükümet düzenlemesi, yaratıcılığı ve İnternet'in gelecekteki gelişimini engelleyebilir. Açık piyasa, seçime dayanır ve kullanıcılar, tekliften memnun kalmazlarsa, İnternet sağlayıcılarını her zaman değiştirebilir. Kullanıcıların seçimi ve piyasa, kötü teklifleri öldürür ve iyi teklifleri sürdürür.

Temel ilkeler

Son yıllarda, politika tartışmaları ve düzenlemeler ağ tarafsızlığı için birkaç temel prensibi kristalize etmiştir:⁵²

- **Şeffaflık:** Operatörler, ortalama bir kullanıcı tarafından anlaşılabilir bir biçimde, ağ yönetimi uygulamaları, kapasiteleri ve hizmetlerinin kalitesi hakkında eksiksiz ve doğru bilgiler vermelidir.
- **Erişim:** Kullanıcılar, [yasal] içeriğe, hizmete veya uygulamaya [düzenleyici tarafından öngörüldüğü gibi anlamlı kullanım için garantili minimum QoS ile] veya ağa zarar vermeyen herhangi bir donanımı bağlamak için [sınırsız] erişime sahip olmalıdır.
- **Ayrımcılık yapmamak:** İşletmeciler, aşağıdakilere dayanarak trafikte hiçbir ayrımcılık [veya yalnızca makul bir ayrımcılık] yapmamalıdır:
 - Göndericinin ve alıcının orijini
 - İçeriğin türü, uygulamanın ve hizmetin türü [Adil rekabet için istenmeyen rakiplerin veya OTT hizmet sağlayıcı servislerine karşı ayrımcılık yapmamak].
 - ‘Makul olan’ sadece şirketlerin avantajına değil (QoS’I güvenceye alma, ağ güvenliği ve esnekliği, yenilikler v e ve daha fazla yatırım, maliyetlerin düşürülmesi vb gibi) kamu yararına da kullanılmalıdır.

Küresel IGF ve Avrupa İnternet Yönetişimi Diyalogu (EuroDIG) gibi uluslararası forumlarda en sık tartışılan diğer ilkeler şunlardır:

- İfade, bilgiye erişim ve seçim özgürlüğünü korumak.
- Minimum QoS ve ağın güvenliği ve esnekliğinin sağlanması.
- Yatırımlar için teşvikleri korumak.
- [yeni iş modelleri ve yenilikçi iş olanakları, yani yeni girenler için fırsatlar dahil olmak üzere] Uyarıcı yenilikler.
- Temyiz ve tazminat hakkı da dahil olmak üzere ilgili tüm tarafların (sağlayıcılar, düzenleyiciler, kullanıcılar) haklarını, rollerini ve hesap verebilirliğini tanımlamak.
- Rekabet karşıtı uygulamaları engellemek.
- Kullanıcıların ağ operatörlerini kolayca seçmelerini ve değiştirmelerini sağlayacak bir piyasa ortamı oluşturmak.
- Engelli insanlar, gelişmekte olan dünyadaki kullanıcılar ve işletmeler gibi dezavantajlıların çıkarlarını korumak.
- İçerik ve servis çeşitliliğini korumak.

Politika yaklaşımları

Ağ tarafsızlığı tartışmasıyla birlikte bir başka soru daha gündeme gelmiştir: yasa koyucuların ve düzenleyicilerin genişbant politikası ve operatör uygulamalarındaki rolü nedir? Düzenleyici-

lerin karşılaştığı en büyük zorluklardan biri, ağ tarafsızlığı ilkesinin olası ihlallerini engellemek için, önceden (ex-ante) etkin davranma veya bir öncüllere dayanarak (ex-post) bir kez (ve eğer) olursa ihlale yanıt vermektir. Yasa koyucuların ve politika yapımcıların karşılaştığı bir diğer zorluk, sorunun ilkeleri yasayla yorumlama demek olan ‘bağlayıcı hukuk’ ile mi ya da kurallar ve politikalarından oluşan ‘bağlayıcı olmayan hukuk’ ile mi çözülmesi gerektiğidir.⁵³

Gelişmiş ülkeler

ABD’de, Federal İletişim Komisyonu (FCC) ağ tarafsızlığından yana bir dizi kuralı kabul etmiştir. Haziran 2015’te yürürlüğe giren kurallar, FCC’nin genişbant hizmetlerini bir imkan olarak düzenlemesine ve kablolu ve kablosuz genişbant sağlayıcılarının, FCC’nin açık İnternet’e zarar vereceğini düşündüğü makul olmayan uygulamaları ortaya koymalarını yasaklamasına imkan vermiştir: Bunlar yasal içeriğin, uygulamaların, hizmetlerin veya aygıtların engellenmesi; içerik, uygulama veya hizmet temelinde yasal İnternet trafiğini zayıflatılması veya azaltılması; ve belirli içeriklerin, uygulamaların veya hizmetlerin önceden ücretlendirilmesidir.⁵⁴ Telekom sağlayıcıları, inovasyon ve altyapıdaki yatırımları olumsuz yönde etkileyebileceklerini iddia ederek mahkemedeki kurallara itiraz ettiler, ancak iddialar Haziran 2016’da federal bir temyiz mahkemesi tarafından reddedildi.⁵⁵ Ancak, sağlayıcıların FCC kuralları aleyhine karşı savaşlarını sürdürmeleri beklenmektedir.

AB düzeyinde, Kasım 2015’te kabul edilen [Açık İnternet erişimine ilişkin Yönetmelik](#), İnternet erişim hizmetleri sağlayıcıları için, internet erişimi hizmeti verirken, gönderici veya alıcıya, erişilen veya dağıtılan içeriğe, kullanılan veya sağlanan uygulama veya hizmetlere veya kullanılan cihaza bakılmaksızın, ayrımcılık yapılmaksızın, kısıtlama yapılmaksızın veya girişime bakılmaksızın tüm trafiğe eşit davranma zorunluluğu getirmiştir.⁵⁶ Düzenleme aynı zamanda ‘uzman servisler’ kavramıyla da ilgilenerek, operatörlerin internete erişim dışında belirli bir içerik, uygulama veya hizmet veya bunların kombinasyonu için düzenlenmiş diğer ‘hizmetleri’ düzenlemenin bu içerik, uygulama veya hizmetlerin belirli bir kalitede sağlanması için gerekli şartları karşılamaya yaradığı durumlarda sağlama imkanı vermiştir.⁵⁷ Ağustos 2016’da, Avrupa Elektronik Haberleşmeleri Avrupa Düzenleyicileri Organı (BEREC), eşit ve dürüst olmayan İnternet erişim hizmetleri ve ilgili “son kullanıcı hakları” temininde trafiğe yönelik ayrımcı muamele açısından AB mevzuatının nasıl uygulanması gerektiğine dair bir rehber yayınlamıştır.⁵⁸

Brezilya⁵⁹, Şili⁶⁰, Slovenya⁶¹ ve Hollanda⁶², ulusal mevzuata göre ağ tarafsızlığını korumaktadır. Öte yandan Norveç, ulusal düzenleyici otorite ağ tarafsızlığı bakımından (ISS’ler, endüstri kuruluşları, içerik sağlayıcılar ve tüketicilerin korunması ajansları gibi çeşitli endüstri oyuncularıyla işbirliği içinde hazırlanan) bir dizi kılavuz ile bağlayıcı olmayan hukuku tercih etmiştir.⁶³

Gelişmekte olan ülkeler

Sınırlı altyapı ve bant genişliği nedeniyle, gelişmekte olan ülkelerin düzenleyicileri, adil kullanım politikasına - uygun fiyatlarla ve herkes için adil erişime daha fazla odaklanmaktadır. Bazıları, sınır ötesi ayrımcılık yasağı konusundaki endişelerini dile getirerek, tüm ülkelerden gelen trafiğin, sonlandırma maliyetlerine dayanan hiçbir tercih olmaksızın aynı şekilde ele alınması

gerektiğini söylemektedir. Ayrıca, bazı ülkeler içsel kültürel, politik veya etik konularda daha fazla hassasiyete sahiptir ki, böylece ‘uygun kullanım’ ve yönetim diğerlerinden farklı olarak anlaşılmaktadır.

Gelişmiş dünyanın yenilikçi modellerinin gelişmekte olan pazarlara köstek olacağı endişeleri ortaya çıkmıştır: büyük İnternet şirketlerinin hizmetlerine öncelik verilmesi, yenilikçiliği, yerel içeriği ve hizmetleri ve medya çeşitliliğini tehdit ederek gelişmekte olan iş ve rekabeti daha da küçültülebilir. Daha önce de belirtildiği gibi, bazı ülkeler sıfır vergi uygulamalarını yasaklayarak ağ tarafsızlığı lehine güçlü konuma gelmeye hazırdılar. Diğer pozisyonlar arasında, ulusal telekomünikasyonların öncelikli olarak küresel OTT’leri ücretlendirmelerine izin verilmesi, böylece mevcut telekomünikasyonların gelirine ilave edilmesi; veya tam tersine, OTT’lerin ABD dışında faaliyet göstermesini sağlamak için ulusal düzeyde net tarafsızlığı uygulama olabilir.

Uluslararası örgütler ve STK’lar

Birçok uluslararası kuruluş ve kullanıcı grubu da ağ tarafsızlığı konusunda politika konumları geliştirmiştir. CoE, 2010’da ağ tarafsızlığı konusundaki Bakanlar Komitesi Deklarasyonu ve 2016’da Bakanlar Komitesi’nin “ifade özgürlüğü hakkını ve ağ tarafsızlığı konusundaki özel yaşam hakkını koruma ve teşvik etme” tavsiyesi kapsamında; İfade ve bilgi özgürlüğü.⁶⁴ İnternet Topluluğu net tarafsızlığa kullanıcı merkezli bir bakış açısıyla yaklaşmakta, çoğunlukla aşağıdaki konulara odaklanmaktadır: ifade özgürlüğüne izin vermek, kullanıcı seçimini desteklemek ve ayrımcılığı önlemek.⁶⁵ ABD ve AB tüketici örgütlerinin bir forumu olan Trans Atlantik Tüketici Diyalogu (TACD) ayrıca, ABD ve AB’yi İnternetin açıklık ve tarafsızlığını ilkelerini korumaya çağıran, ayrımcı olmayan taşıyıcı davranış taleplerine de vurgulamaktadır.⁶⁶ Ağ tarafsızlığı ve çok katmanlı bir internet WCIT-12 sürecinde yoğun bir şekilde tartışılmıştır.⁶⁷ 2014’teki son NET- belediye belgesi, kabul edilen ilkeler arasında net tarafsızlığı içermiyor, ancak özellikle IGF içinde, konuyla ilgili daha fazla tartışma başlattı.

Birçok STK, özellikle ticari olmayan ve ticari olmayan çevrimiçi içerik ve hizmetlerin geleceğinden endişe duymakta, bunların ticari olanlara eşit herhangi bir taşıyıcı ağ üzerinden yayınlanmasını istemektedir. Ayrıca, marjinalleşmiş grupların - özellikle de engelli kişilerin - içeriklerini, hizmetlerini ve uygulamalarını (yüksek bant genişliği gerektirenler de dahil olmak üzere) ihtiyaçları için herhangi bir sınırlama olmaksızın kullanma hakları üzerinde dururlar.

Açık meseleler

Ağ tarafsızlığı tartışma gündeminde bir dizi açık konu bulunmaktadır:

- Denge, bir yandan İnternetin kamu yararı ile kullanıcı (ve insan) hakları, diğer yandan da sağlayıcıların sahip oldukları ağlarda inovasyon hakları arasında denge nerede olmalıdır?
- Açık rekabete sahip olmayan düzenlenmiş bir piyasa, taşıyıcıların savunduğu gibi, kullanıcılar için sınırsız (veya yeterli) bir seçenek sağlar mı?⁶⁸ Kullanıcılar da anlamlı kararlar verebilecek mi? Yoksa düzenleyiciler kaçınılmaz olarak bekçi gibi güçlendirilmeli, eğer öyleyse hangi yetkiyle yetkilendirilmeli?

- Farklı yasal ve düzenleyici yaklaşımlar geniş bant piyasasını ve daha fazla yatırım ve inovasyonu nasıl etkiler?
- Gelişmekte olan dünya açısından net tarafsızlığının etkileri nelerdir?
- Katmanlı bir internetin rekabet, inovasyon, yatırım ve insan hakları açısından etkileri nelerdir?
- Sıfır - derecelendirme tarifeleri veya CDN'lerin geliştirilmesi "katmanlı Internet" olarak değerlendirilmeli midir?
- Hem içerik hem de servis sağlayıcılar olarak baskın OTT katmanlı bir İnternet ve olası yeni hizmetleri de kazançlı bir iş modeli olarak bulacak mı? Bu durumda, onu geliştirmekte olan ülkelerin kullanıcılarını içerecek şekilde adapte edebilecekler mi, yoksa bu ülkeleri dışarıda bırakılacaklar mı?
- Telekom operatörleri (iTunes, Google ve diğer OTT servis sağlayıcılarının başarılı örneklerini ve OTT servis sağlayıcıları ve operatörleri arasındaki ortaklık potansiyeli gibi başarılı örnekleri izleyerek) net tarafsızlığını ihlal etmeden gelirlerini artırmak için iş modellerini geliştirebilirler mi?
- Kalite gibi teknik nedenlerden ötürü trafik yönetimi ihtiyacı, taşıyıcı teknolojisindeki gelişmeler nedeniyle gelecekte modası geçmiş olacak mı?
- Bulutlara ve NesNet'e olan artan bağımlılık, ağ tarafsızlığı üzerindeki veya ağ tarafsızlığı artan bağımlılık üzerindeki tartışmaları nasıl etkileyecektir?
- Tartışma, taşıyıcı düzeydeki trafik yönetiminden Google, Apple veya Facebook gibi içerik ve uygulama sağlayıcı içerik ve uygulama yönetimi seviyesine mi evrilecektir?
- Tüketici koruması, doğal olarak ağ tarafsızlığıyla bağlantılı olmaya devam edecek mi?
- Ağ tarafsızlığı "kaybederse", gelecekte tüketicinin korunmasını hangi ilkeler destekleyecektir?

www.igbook.info/netneutrality

Teknik ve web standartları

Teknik standartlar

İnternet teknik standartları, çeşitli kuruluşlar tarafından geliştirilen veya üretilen donanım ve yazılımların yalnızca İnternet'e bağlanmasını sağlamakla kalmaz, aynı zamanda mümkün olduğu kadar sorunsuz çalışmasını sağlar. Bu nedenle standartlar, birlikte çalışabilir donanım ve yazılım geliştirmeleri için üreticiler dahil teknik topluluğa yön gösterir. Daha önce açıklandığı gibi, TCP/IP İnternet'in ana teknik standardıdır.

Teknik altyapı standartlarının oluşturulması

Standardizasyon süreci herhangi bir sektörde çok uzun olabilir. ICT şirketlerinin yeni teknolojileri hızlı bir şekilde uyguladıkları için, ITU gerçek zamanlı koşullara adapte olmak zorunda

kalmış ve böylece standardizasyon iş akışını birkaç aya sıkıştırmıştır. Yine de, bazı önemli standartların kabul edilmesi yıllar alabilir. Örneğin, ITU, sözde 5G şebekelerinin 2020 yılına kadar standartlaştırılmasını ummaktadır.⁶⁹

ITU'nün yanı sıra, teknik standartlar giderek daha fazla özel ve meslek kuruluşları tarafından belirlenmektedir. İnternet Mimarisi Kurulu (IAB), İnternet'in teknik ve mühendislik gelişimini yönetirken, çoğu standart yorum talebi (RFC) olarak IETF tarafından belirlenmektedir. Hem IAB hem de IETF, İnternet Topluluğunda kurumsal yere sahiptir.

Diğer kurumlar arasında **WiFi standardı** (IEEE 802.11b) gibi standartlar geliştiren Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE); WiFi uyumlu ekipman için sertifikasyon kuruluşu olan WiFi Alliance; ve mobil ağlar için standartlar geliştiren Groupe Speciale Mobile Association (GSMA) bulunmaktadır. Bu kadar hızlı gelişen bir pazarda standartlar koymanın ya da uygulamanın işlevi bu kurumlara kayda değer bir güç vermektedir.

Açık olan standartlar (açık İnternet standartları), geliştiricilerin izin almaksızın yeni servisler oluşturmasını sağlar. Örnekler, www ve bir dizi İnternet protokolünü içerir. Standartların geliştirilmesine açık yaklaşım, birkaç kurum tarafından onaylanmıştır. Açık Standart girişimi, örneğin, açık ve küresel pazar odaklı standartların geliştirilmesini teşvik eder ve IEEE, IETF, IAB ve İnternet Topluluğu gibi kuruluşlar tarafından desteklenmektedir.

Teknoloji, standartlar ve politika

Bu kadar hızlı gelişen bir pazarda uygulama standartlarının belirlenmesinde rol almak standart belirleme kuruluşlarına önemli miktarda güç sağlamaktadır.

Teknik standartlar, ekonomik ve sosyal sonuçlara ulaşmada, özel çıkarları desteklemekte ve rakip işletmeler ve/veya ulusal çıkarlar arasındaki güç dengesini değiştirmeyi sağlayabilir. İnternet için standartlar şarttır. İnternet geliştiricileri, standartlar ve yazılım tasarımı sayesinde, örneğin (bilgi özgürlüğü, gizlilik ve veri koruması gibi) insan haklarının nasıl kullanılacağını ve korunacağını şekillendirebilir.

Resmi standartlar oluşturma çabaları, sistem üreticileri tarafından verilen özel teknik kararları kamusal alana taşımaktadır; standart mücadeleleri bu şekilde, zımni varsayımları ve çıkar çatışmalarını aydınlatılabilir. Paydaşların standart kararlarına itiraz etme tutkusu bizi somun ve civatadan daha derin konulara sürüklemelidir.

Web standartları

Web standartları, www için resmi standartlar ve teknik özellikler kümesidir. İçeriğin cihazlar ve yapılandırmalar arasında erişilebilir olmasını sağlar ve bu nedenle web siteleri ve İnternet uygulamaları geliştirmek için temel kuralları koyar. Ana içerik ve uygulama standartları arasında, belgenin yapısını tanımlamak için etiketleri kullanan düz bir metin dili olan HTML (HTML5, HTML standardının beşinci ve güncel sürümüdür); yapılandırılmış bilgiyi paylaşmak için kullanılan başka bir dil türü olan XML; Web sayfalarının sunumunu kontrol etmek için HTML

ile birlikte kullanılan bir dil olan Basamaklı Stil Sayfaları (CSS); ve daha katı kurallar kullanan genişletilmiş bir HTML sürümü olan XHTML yer almaktadır.

Web standartlarının evrimi

1980'lerin sonunda, ağ standartları mücadelesi sona ermişti. Açık Sistemler Bağlantı mimarisinin bir parçası olan ITU destekli X-25 ve IBM'in sistem ağı mimarisi (SNA) gibi pek çok özel standart gibi diğer standartları marjinalleştiren, TCP/IP giderek ana ağ protokolü haline gelmiştir. İnternet, TCP/IP üzerinden çeşitli ağlar arasında normal iletişimi kolaylaştırırken, sistem hala ortak uygulama standartlarından yoksun haldeydi.

Tim Berners - Lee ve Cenevre'deki Avrupa Nükleer Araştırmalar Örgütü'ndeki (CERN) meslektaşları tarafından, İnternet üzerinden bilgi paylaşımı için (Uluslararası Standardizasyon Örgütü'nün (ISO) SGML olarak adlandırılan mevcut standartlarının sadece basitleştirilmiş bir şekli olan) HTML denilen yeni bir standarttan oluşan bir çözüm geliştirmişlerdir. İnternette ilk olarak görüntülenen içeriğin HTML standartlarına göre düzenlenmesi gerekmiştir. HTML, www'nin temeli olarak, İnternet'in katlanarak büyümesinin yolunu açmıştır.

İlk versiyonundan bu yana, HTML sürekli yeni özellikler eklenerek geliştirildi. İnternetin artan önemi, HTML'nin standartlaştırılması sorununu odak noktası haline getirmiştir. Bu, özellikle Netscape ve Microsoft'un HTML standartlarını etkileyerek pazardaki konumlarını güçlendirmeye çalıştığı Tarayıcı Savaşları sırasında önem arz ediyordu. Temel HTML yalnızca metin ve fotoğrafları işlerken, daha yeni İnternet uygulamaları, veritabanlarını, videoyu ve animasyonu yönetmek için daha gelişmiş teknolojilere ihtiyaç duyuyordu. Bu tür çeşitli uygulamalar, İnternet içeriğinin İnternet tarayıcılarının çoğu tarafından düzgün bir şekilde görüntülenebilmesi için önemli bir standardizasyon çalışması gerektirmiştir.

Uygulama standardizasyonu, internet içeriği için standartların belirlenmesinde daha fazla esneklik sağlayan XML'in ortaya çıkmasıyla yeni bir aşamaya girmiştir. Yeni XML standartları getirilmiştir. Örneğin, kablosuz içeriğin dağıtımı için standarda Kablosuz İşaretleme Dili (WML) adı verilmiştir.

Web standartlarını belirleme

Ana web standardı geliştirme kurumu, Tim Berners - Lee başkanlığındaki W3C'dir. Standartlar, fikir birliğini, doğruluğu, kamu sorumluluğunu ve kaliteyi arttırmayı amaçlayan ayrıntılı bir süreçle geliştirilir. Mutabakata varıldıktan sonra, standartlar Öneriler şeklinde yayınlanır.⁷⁰

W3C standartları, uygulamaların geliştirilmesi için geliştiricilerin zengin etkileşimli deneyimler oluşturmalarını sağlayan açık bir platformu tanımlamaktadır. W3C, 'platformunun sınırları gelişmeye devam etmesine rağmen, endüstri liderleri, HTML5'in bu platformun temel taşı olacağı konusunda neredeyse tamamen ortak düşünmekte' olduğunu ifade etmiştir.⁷¹

İnternete olan ilgisinin yüksek olmasına rağmen, şu ana kadar W3C'nin İnternet yönetimi tartışmasına fazla dikkat çekmemiş olması dikkat çekicidir.

www.igbook.info/standards

Bulut bilişim

Bulut bilişim nedir ve nasıl çalışır?

Bulut bilişim (Şekil 9), bilgisayarlarımızdaki sabit disklerdeki verileri depolamak yerine bunları bulutlardaki sunucularda depolamaya (yani, büyük sunucu çiftliklerine) kaydırmak olarak tanımlanabilir. Bulut bilişim, dünyanın herhangi bir yerindeki herhangi bir cihazdan (İnternet bağlantısının olduğu yerlerde) verilerimize ve servislerimize her zaman her yerde erişim sağlar. Aynı zamanda, verilerimizin üçüncü bir tarafla birlikte depolanması - çoğu zaman çeşitli bölgelere dağılmış parça ve kopyalarda - mahremiyet ve verilerin korunmasına ilişkin kaygılar doğurmaktadır. Bulut sistemindeki güvenlik ihlalleri büyük miktarda verilere erişim sağlayabildiğinden, bulutun güvenliği kendi bilgisayarlarımızdan çok daha yüksek bir seviyededir.

İlk bulut bilişim dalgası çevrimiçi posta sunucularının (Gmail, Yahoo!), sosyal medya uygulamalarının (Facebook, Twitter) ve çevrimiçi uygulamaların (Wikis, bloglar, Google Dokümanlar) kullanımıyla başlamıştır. Gündelik uygulamaların yanı sıra, bulut bilişim iş yazılımları için yaygın olarak kullanılmaktadır. Dijital varlıklarımızın giderek daha fazlası sabit disklerimizden buluta geçmektedir. Bulut bilgi işlemdeki ana oyuncular, zaten büyük sunucu çiftlikleri olan veya bunları geliştirmeyi planlayan Google, Microsoft, Apple, Amazon ve Facebook'tur.

Bir şekilde, bulut bilişim, bilgisayar teknolojisinin gelişiminde bir çember kapattı. Bilgisayarların ilk günlerinde, güçlü ana bilgisayarları ve 'aptal' iş istasyonları vardı. Güç, merkezde, güçlü sunuculardaydı. Gücün güçlü sunuculardan son kullanıcı terminallerine geçmesi, IBM, Apple ve Microsoft gibi şirketler kişisel bilgisayarlar üretmeye başladıklarında gerçekleşmiştir. Bilgisayar gücü dünya çapındaki şirketlere yöneldi. Bilgisayarlarımızda disket ve sabit disklerde veri depolamaya ve uygulamaları (metin işlemcilerden oyunlara) çalıştırmaya. Daha sonra ağ teknolojileri bu bireysel bilgisayarları önce şirketler ve kuruluşlar (Yerel Alan Ağları, Yerel Ağlar aracılığıyla) ve daha sonra genel olarak, özellikle de İnternet üzerinden bağlamaya başladı. İnternetin kamusal büyümesinin ilk evresinde (2005 yılına kadar), İnternet çoğunlukla veriler bilgisayarlarda depolanırken veri alışı verişinde kullanılırken, kelime işlemesi gibi temel yazılımlar da internet üzerinden yürütülmüştür.

Son 10 yılda sosyal medyanın büyümesi ve akıllı telefonların ve tabletlerin ortaya çıkmasıyla bir başka değişim başladı. Buna paralel olarak, yazılım ve veriler bilgisayarlarımızdan buluttaki güçlü sunuculara geçmeye başladı. Bu işlem, Gmail gibi e - posta hizmetleriyle başladı ve fotoğraflarımızı, metin dosyalarımızı ve diğer dijital kaynaklarımızı bulutta depolamaya ve yazılımı bulutta da çalıştırmaya devam etti (Google Docs veya Microsoft Office 365 gibi). Bugün, dijital varlıklarımızın çoğu buluttaki merkezi sunucularda depolanmaktadır. Bir şekilde, merkezi olmayan bir kişisel bilgisayar aracılığıyla, merkezi bir ağ oluşturma mimarisinden, buluttaki merkezi depolamaya kadar ilerlemiş olduk.



Şekil 9. Bulut bilişim

Bir bulut kurulumu üç katmandan oluşur: donanım, ara katman yazılımı veya platform ve uygulama yazılımı. Kullanıcı tarafından kiralananlara göre, üç tür bulut hizmeti vardır:

- Bir bulut sağlayıcının, kullanıcıya yazılım uygulamalarına erişim sağladığı ve böylece İnternet'e bağlı herhangi bir cihazdan kullanıcının bu tür uygulamalara (ve bunlar aracılığıyla üretilen verilere) erişmesini sağlayan bir **Hizmet Olarak Yazılım (veya SaaS)**. Burada, kullanıcının bulut kaynaklarının hiçbiri üzerinde kontrolü yoktur, ancak yalnızca mevcut uygulamayı kullanabilir. Bu, son kullanıcı uygulamasının kullanım için bir giriş noktası olduğu en baskın hizmet türüdür - Twitter ya da yerel organizasyondaki merkezi veritabanı için bir uygulama gibi.
- Kullanıcının, kiralık bulut platformunda çalışacak bir uygulama geliştirebileceği bir **Hizmet Olarak Platform (veya PaaS)**. Bu şekilde, kullanıcı kullanmak istedikleri donanım kaynaklarına karar verebilir; yine de sunucuyu veya depolama ayarını ayarlama olanağına sahip olmayacaklardır. Standardizasyon özellikle platform açısından önemlidir, çünkü geliştiricilerin çok çeşitli potansiyel müşterilere hitap etmelerini sağlar ve kullanıcılara seçenek sunar.
- Bir **Hizmet Olarak Altyapı (veya IaaS)**, daha geniş popülasyonlar arasında en az kullanılan bulut hizmetidir, çünkü gelişmiş BT becerileri gerektirir, ancak kaynakları nasıl kullanacağını seçmede en yüksek özgürlüğü sağlar. IaaS'de, sağlayıcı yalnızca donanım kaynakları (he-

saplama gücü veya depolama) sağlarken, kullanıcının işletim sistemi de dahil olmak üzere hizmetleri kurması gerekir.

Bulut bilişim ile ilgili hukuki konular ve politika konuları

Kritik bilgi altyapısı olarak bulut sunucuları

Çoğu İternet uygulaması bulut sunucularından çalışır. Bulut öncesi dönemde, İternet kesildiğinde hasar, hizmetin bulunmamasının yetersizliği ile sınırlıydı - e-posta gönderemedik veya web'e göz atamadık gibi. Bulut bilişim çağında, bu görevler bulut tabanlı uygulamalar yoluyla gerçekleştirildiğinden, metin yazamayabilir veya hesaplamalar yapamayabiliriz. Milyonlarca İternet kullanıcısı ve firması için bulut hizmetlerinin yüksek ilgisi, bulut sunucularını küresel düzeyde ve dünya çapındaki çoğu toplumda kritik altyapıların bir parçası haline getirir.

Güvenlik ve şifreleme

Tek bir bulut operatörünün binlerce veya milyonlarca insana hizmet sağlaması, kırılganlıklardan yararlanmak isteyen, suçlular, teröristler, siber casuslar veya diğer kanun dışı kişilerin dikkatini için çekmek için yeterlidir.

Bulutun olası güvenlik açıkları, bilgi güvenliği üçlüsü olarak bilenen - verilerin gizliliği, bütünlüğü ve verilerin ve sistemin kullanılabilirliğine (CIA) göre kategorize edilebilir. Bu amaçla, bulutun güvenliğini sağlamak, belirli veri ve hizmet bölümlerine erişim haklarına karar vermek, buluttaki tüm veri kümesini şifrelemek, BİT sisteminin her bir bölümünü güvenceye almak gibi bir dizi önlemin değerlendirilmesini içerecektir. Bulut ile kullanıcılar arasındaki ağ, bulut ve son kullanıcılar arasındaki veri aktarımını şifreleyerek ve bulutta depolanan tüm verileri yedekler (Şekil 10).

veriler, otomobillerin, evaletlerinin ve hatta giysilerimizin bile veri toplamaya başlayacağı nesnelerin İnternetinin hızla büyümesiyle yeni bir boyut kazanacaktır. Büyük veri yeni ekonomik modelleri tetikleyecektir. Bulut kaynaklarına olan talebi de tetikleyecektir.

Örneğin, sis bilişim, buluta işlenmek ve analiz edilmek için aktarılan verinin miktarının azaltmak için bulut bilişime ek olarak geliştirilmektedir. Cisco tarafından açıklandığı gibi, sis bilişimi, bulutu, veri üreten ve bunlar üzerinden çalışan “nesnelere” daha yakın hale getirir; Bu, verilerin toplandığı veya üretildiği yere daha yakın yerde analiz edilmesini sağlar, böylece gecikmeyi⁷² en aza indirir, gigabaytlar tutarındaki ağ trafiğini çekirdek ağdan boşaltır ve hassas verileri ağ içinde tutar.⁷³

Verilerin yerelleştirilmesi

Dijital bilgi varlıklarının gittikçe artmasıyla birlikte, ülkeler ulusal veri varlıklarının ulusal sınırların dışında olması konusunda rahatsız olmaktadır. Bazıları (bulut servis sağlayıcılarına ve/veya ulusal sınırlar dahilinde depolanacak verilere ilişkin) veri yerelleştirme kurallarını benimsemekle ya da yerelleştirme olasılığını araştırmaktadır.

Verinin yerelleştirilmesine ilişkin motivasyonlar ekonomikten siyasete kadar değişmektedir. Ekonomik verilerin yerelleştirilmesi genellikle korumacı bir ekonomik politikaya dayanmaktadır. Veriler İnternet ekonomisinin kilit kaynağı ise, ülkeler bu kaynağı kendi topraklarında korumaya ve veri işleme ve yönetimine dayanan yerel bir ekonominin gelişimini desteklemeye çalışmaktadır. Veri koruma ve güvenlik hususları ayrıca hükümetleri belirli verilerin yalnızca ülke içinde işlenmesini ve saklanmasını gerektirdiğinden, ulusal mevzuatı doğrudan servis sağlayıcılara uygulanabilir kılabilir. Ayrıca, ülkeler ayrıca hükümet/resmi verilerin işlenmesi ve depolanması için özel olarak tasarlanmış hükümet bulutlarının kurulması fikrini keşfetmeye başlamıştır. Veri yerelleştirme politikalarının politik nedenleri, bazı ülkelerin siyasi aktivizmi kontrol etme konusundaki çıkarlarıyla bağlantılıdır; bu durum ülkenin veri sunucuları üzerinde yargı yetkisine sahip olması halinde daha kolay oluşabilir.

Bulut servis sağlayıcıları, müşterilerine bulut hizmetlerinden yararlanma imkanı sunarken, yerelleştirme politikalarını aşmak için teknik olanlar da dahil olmak üzere çözümler bulmaya çalışmaktadır. Örneğin, Mart 2016’da Oracle, şirketlerin Oracle bulut sunucularını kendi veri merkezlerine yerleştirmelerini sağlayacak yeni bir bulut bilişim hizmeti başlattı. Oracle’a göre, yeni hizmet şu ana kadar bulut bilişimi bulut sunucularının konumuyla ilgili yasal veya düzenleyici gereksinimler yüzünden kabullenmeyen kuruluşların gereksinimlerine yanıt vermek için tasarlanmıştır.⁷⁴

Standartlar ve birlikte çalışabilirlik

Çeşitli bulut bilişim operatörleriyle birlikte, standartlar sorunu çok önem kazanmaktadır. Standartlar birlikte çalışabilirlik ve verilerin farklı bulutlar arasında (örneğin Google’dan Apple’a) aktarılması için özellikle önemlidir. Tartışılmakta olan bir olasılık, bulut bilişimdeki temel aktörler tarafından açık standartların kabul edilmesidir. Ancak bunu başarmak kolay değil-

dir, çünkü büyük bulut bilişim şirketleri ticari standartlarını rekabet avantajlarının bir parçası olarak görmektedir. Bununla birlikte, birlikte çalışabilirliği sağlamaya yönelik çeşitli girişimler bulunmaktadır.

Örneğin, 2013 yılında, Open Group (Fujitsu, IBM ve Oracle gibi üyeleriyle birlikte), bulut ürünleri ve hizmetleriyle çalışırken nasıl taşınabilirlik ve birlikte çalışabilirlik elde edileceği konusunda kullanıcılara ve aynı zamanda tedarikçilere ve standartlara, daha iyi taşınabilirlik ve birlikte çalışabilirlik sağlamak için standartların ve en iyi uygulamaların nasıl gelişmesi gerektiği konusunda tavsiyelerde bulunan **Bulut Bilişim Taşınabilirlik ve Birlikte Çalışabilirlik Kılavuzu**'nu yayınlamıştır.⁷⁵ IEEE, diğerlerinin yanı sıra, bulutlararası birlikte çalışabilirlik için standartlar geliştirmek üzere çalışan IEEE Bulut Bilişim İnisiyatifini kurmuştur.

www.igbook.info/cloud

Nesnelerin İnterneti

Nesnelerin İnterneti (NesNet), İnternet bağlantısını (bilgisayarlar, cep telefonları, tabletler ve e - okuyucuları gibi) bilgi ve iletişim cihazlarından öteye arabalar, evaletleri, giysiler, şehir altyapısı, tıbbi ve sağlık cihazları gibi diğer cihazlara doğru genişletmektedir.

2020 yılına kadar NesNet'e bağlı cihazların sayısı için tahminler 20 ile 100 milyar arasında değişmektedir. Bu cihazlar analiz için özellikle değerli olan önemli miktarda veri üretecektir. Uluslararası Veri Şirketi (IDC), 2020'de "dijital evrenin" 44 ZB'ye (zettabayt, yani trilyon gigabayt) ulaşacağını ve bu miktarın% 10'unun NesNet cihazlarından geleceğini tahmin etmektedir.⁷⁶

NesNet endüstrisinin finansal gelişiminin öngörülleri artmakta ve üreticilerin planları roket gibi hareket etmektedir. Verizon, dünya genelindeki NesNet pazarının önümüzdeki birkaç yıl içinde, 2014 yılında 591,7 milyar dolardan 2019'da yıllık% 17'lik bir büyüme oranı ile 1,3 trilyon dolara kadar artacağını tahmin etmektedir.⁷⁷

ITU ve Cisco Systems tarafından 2016 yılı başında yayınlanan bir rapor, NesNet'in dünyadaki yaşam standartlarını iyileştirebilecek ve sürdürülebilir kalkınma hedeflerine ulaşmada önemli katkı sağlayan önemli bir gelişme fırsatı olduğu sonucuna varmaktadır. Rapor, NesNet'in sağlık, eğitim, su ve hıfzıssıha, iyileşme, iklim değişikliği ve kirlilik azaltma, doğal kaynak yönetimi ve enerji gibi alanlarda artan etkisinin ana hatlarını çizmektedir.⁷⁸

NesNet cihazları genellikle "akıllı evler" veya "akıllı şehirler" olarak tanımlanan geniş sistemlere bağlanır. Bu tür cihazların her ikisi de muazzam miktarda veri üretir ve verilerin kullanıldığı yeni metinler oluşturur. NesNet cihazları mevcut İnternet yapısını kullanır, ayrı veya farklı bir İnternet kullanmaz.

NesNet cihaz iletişimi için şu anda kullanılan en yaygın sensörler ve parçalar şunlardır:

- Radyo Frekansı tanımlayıcıları (RFID'ler): izlemeyi etkinleştirmek için öğelere eklenmiş elektronik etiketler. Giysi, evcil hayvan, kutu nakliye veya takip için uygundur.
- Evrensel Ürün Kodları (UPC'ler): Neredeyse tüm ürünlerde, UPC'ler süpermarket kasası taramasında kullanılır.

- Elektronik Ürün Kodları (EPC'ler): dünyanın herhangi bir yerindeki her fiziksel nesne için her zaman benzersiz bir kimlik sağlar. EPC'ler UPC'ler gibi işlev görür, ancak elektrondur.

Buna ek olarak, araştırmacılar NesNet cihazlarını bağlamak için diğer yöntemleri keşfetmeye devam etmektedir. Örneğin, Haziran 2016'da yayınlanan bir makalede⁷⁹, bir grup araştırmacı NesNet'deki cihazları bağlamak için Işık Yayan Diyot (LED) ampullerin kullanılmasını önermektedir. Böyle bir sistemin (birçok NesNet cihazının artık radyo frekanslarının kullanımına bağlı olduğu göz önüne alındığında) doymuş radyo spektrumundaki iletişim zorluklarına bir çözüm olabileceğini savunmaktadırlar.

Bağlı NesNet cihazları tarafından üretilen tek bir veri parçasının boyutu oldukça küçük olsa bile, bağlanabilecek cihazların sayısı ve verilerin bulutta saklanıp işlenebilmesi nedeniyle son toplam şaşırtıcıdır. Bu nedenle, bulut bilişim endüstrisi, gelecekteki NesNet gelişmelerinde önemli bir rol oynayacaktır.

NesNet endüstrileri

En gelişmiş NesNet endüstrilerinin bazıları şunlardır:

- **Ev otomasyonu:** Ev aletlerine her yerden erişim sağlama. Birleşik bir protokol veya endüstri web API standardı yoktur.
- **Sağlık izleme:** (doktorlar uzaktan ayarlanan insülin pompaları, kalp pili izleme gibi konular-da) sağlığını aktif olarak ayarlar . Döngüleriniz veya alışkanlıklarınızla ilgili veri oluşturur, ancak birçok olası güvenlik sorunu ve rastgele veri yükleme söz konusudur.
- **Ulaşım:** Yakıt kullanımı, konum, süre, mesafe gibi bilgileri takip etmek ve ayrıca (filolar dahil) araçlardaki bakım ihtiyaçlarını önceden tahmin etmek ve kaynak kullanımını optimize etmek için NesNet sistemlerinin kullanılması. Birkaç adım öteye gidersek, şu anda (Tesla ve Toyota gibi) otomobil üreticileri tarafından keşfedilen kendi kendini süren otomobillerin yanı sıra Google ve Uber gibi şirketler de NesNet teknolojilerini kullanmaktadır.

NesNet'nin artan bir rol oynadığı diğer endüstriler arasında enerji, altyapı, tarım, üretim ve tüketici uygulamaları yer almaktadır. (BİT'lerin, kalitelerini ve performanslarını iyileştirmek ve genel şehir yaşamı standartlarını artırmak için kentsel hizmetlere ve altyapılara entegre edildiği) akıllı şehirlerin genel konsepti NesNet ile de güçlü bir şekilde ilişkilidir.

Özel ve kamu sektörü inisiyatifi

İş dünyası büyük NesNet girişimlerine liderlik etmektedir. Cisco ve Intel gibi teknoloji şirketleri NesNet servislerinin portföylerini geliştirmeye devam ederken, telekomünikasyon hizmet sağlayıcıları NesNet kullanımına teşvik etmek için NesNet'ye özel ağları daha geniş bir ölçekte kullanmaya başlamışlardır.⁸⁰ Ayrıca, farklı sektörlerden şirketler de, NesNet alanındaki gelişmelere daha fazla katkı sağlamayı amaçlayan ittifaklar şeklinde güçlerini birleştirmektedir. Bunun bir örneği, NesNet cihazlarının üreticiden, işletim sisteminden, yonga setinden veya fiziksel taşımacılığa bakılmaksızın birbirleriyle iletişim kurabilmelerine katkıda bulunmak olan Açık

Bağlantı Vakfıdır. Vakıf, otomotiv, tüketici elektroniği, sağlık, sanayi vb. gibi çeşitli sektörlerden üyeler içermektedir. Diğer bir örnek ise NesNet standardizasyonu alanında çalışan LoRa (İttifakı) Alliance'dır. İttifak, NesNet nesneleri arasında kesintisiz birlikte çalışabilirlik sağlamayı amaçlayan Düşük Güçlü ve Geniş Alanlı Ağları (LPWAN) özelliği olan LoRaWAN'ı geliştirmiştir.

Hükümetler, NesNet'nin getirdiği fırsatların giderek daha fazla farkında hale gelmektedir. Bu alanda çeşitli girişimler başlatmaktadır. Örneğin, AB, Avrupa'da NesNet'nin alımını teşvik etmeyi amaçlayan bir finansman programı olan Horizon 2020 Çalışma Programı 2016/2017: Nesnelerin İnterneti Büyük Ölçekli Pilot Testleri ve Uygulaması başlatmıştır. ABD'de, NTIA, özel sektör ile ortaklaşa çalışarak NesNet teknolojilerinin gelişmesini sağlamada federal hükümetin olası rollerini belirlemeye çalışırken, NesNet'in teknolojik ve politika ortamını incelemektedir. Çin hükümeti, NesNet ile ilgili çeşitli alanlarda araştırmaları finanse ettiği Chengdu Nesnelerin İnterneti Teknoloji Enstitüsü'nü kurmuştur.

Temel Meseleler

NesNet çok büyük miktarda veri üretir ve bu da gizlilik ve veri koruması ile ilgili önemli endişeleri tetikler. Bazı (tıbbi NesNet cihazları gibi) NesNet cihazları, kişisel niteliklere sahip veri toplayabilir ve aktarabilir ve cihazların nasıl korundukları (güvenliği nasıl sağladıkları)⁸¹ ve bunun yanı sıra toplanan ve analiz edilen verilerin nasıl korunacağı konusunda endişeler vardır. Bir NesNet cihazı tarafından iletilen bilgiler gizlilik sorunlarına yol açmayabilirken, birden fazla cihazdan toplanan veri kümeleri bir araya getirildiğinde, işlendiğinde ve analiz edildiğinde, bu hassas bilgilerin açık hale gelmesine neden olabilir.

Verilerin yönetilememesi, aynı zamanda verilerin mülkiyeti konusunu da gündeme getirmektedir. NesNet'te kullanılan birçok uygulama, yaratılan veriler ve bunlar arasında üretilen veriler mülkiyet hakkını içerir. Veri, protokol ve cihazların güvenliği ve mahremiyetinin sağlanması yeni düzenlemelere ihtiyaç duyulabilir. Bu birleşik, küresel bir eylem ve düzenleme gerektiren, belki de İnternet yönetişi alanındaki herhangi bir şeyden daha fazlasını gerektiren gelecekte ortaya çıkacak bir gelişmedir. Yeni sosyal sözleşmelerde de anlaşmaya varılması gerekir.

Robotları, kendini süren arabaları ve yargı ve kararlar vermek zorunda olan diğer dijital sistemleri tanıtmak isteyen yapay zeka girişimlerinin merkezinde bulunan NesNet ile etik konular ortaya çıkmıştır. Hükümetler ve özel sektör NesNet ve AI alanlarındaki gelişmelere etik ilkelerin uygulanması gerektiği ve bu ilkelerin NesNet ve AI sistemlerine nasıl dahil edilebileceği konusunda giderek daha fazla diyalog çağrısı yapmaktadırlar.

Etik meseleler

NesNet, büyük veri ve AI, etik meseleleri dijital politikanın odağına yerleştirmektedir. Etik kaygılar yalnızca gizlilik ve güvenlik ile değil aynı zamanda otomatik makinelerin verdiği kararların etik olup olmadığı ile de ilgilidir. Örneğin, bir Google iştiraki olan Jigsaw, İnternette suistimal ve tacizi tespit etmeyi amaçlayan bir dizi araç olan **Conversation AI**'yi geliştirmiştir. İnternet kamusal alanın kötüye kullanılması ile ilgili problemleri ele alırken, yazılım aynı zamanda önemli bir etik sorun ortaya çıkarmaktadır: Makineler neyin uygun neyin uygun olup olmadığını nasıl belirleyebilir?⁸²

Yeni dijital teknolojilerin etik etkileri üzerine tartışmalar hem iş dünyasında hem de politika oluşumunda başlamıştır. Başlıca (IBM, Facebook, Google, Microsoft, Amazon ve Deep-Mind gibi) İnternet şirketleri, AI'nın gizliliğini, güvenliğini ve etik zorluklarını ele almayı ve yeni dijital gelişmelerin etik meseleleri hakkında daha geniş bir sosyal diyalogu başlatmayı amaçlayan bir Yapay Zeka Ortaklığı girişimi başlatmıştır.⁸³ Avrupa Parlamentosu'nda 2016'nın ilk yarısındaki robotek konusunda hazırlanan taslak bir rapor robotik alanındaki teknolojik gelişmelerin getirdiği etik zorlukları incelemekte ve robotların tasarımı, üretimi ve kullanımının 'onur, insanlık onuru ve özerklik, ayrıca insanlık onuru ve insan hakları, adalet ve eşitlik, ayrımcılık yapmama ve damgalanmama [...] gibi ilkelere ' [...] dayanması' gerektiğine ilişkin bir çerçeveyi' kabul etmiştir.⁸⁴ ABD'de Ekim 2016'da yayımlanan **Ulusal Yapay Zeka Araştırma ve Geliştirme Stratejik Planı**, 'etik muhakemeyi içeren AI sistemleri için en iyi tasarım mimarisinin nasıl olacağını belirleme' ihtiyacını vurgulamaktadır.⁸⁵ Robotik ve İngiltere Parlamentosu'ndaki Bilim ve Teknoloji Komitesitarafından hazırlanan bir rapor hükümeti AI gibi özerk teknolojilerin kullanımıyla ilgili etik sorunların üstesinden gelmek için proaktif önlemler almaya çağırılmaktadır.⁸⁶

www.igbook.info/NesNet

Yakınsama

Tarihsel olarak, telekomünikasyon, yayın ve diğer ilgili alanlar ayrı sektör bölümleriydi; farklı teknolojiler kullandılar ve farklı düzenlemelere tabi tutuldular. İnternetin genel ve yaygın kullanımı, telekomünikasyon, yayın ve bilgi sunumu için var olan teknolojik platformların yakınlaşmasına yardımcı olmuştur. Bugün internet üzerinden telefon görüşmeleri yapabilir, TV izleyebilir, bilgisayarlarımızda müzik paylaşabiliriz. Sadece birkaç yıl önce, bu tür hizmetler farklı teknolojik sistemler tarafından yerine getirildi.

Geleneksel telekomünikasyon alanında, yakınlaşmanın ana noktası VoIP'dir. Skype, WhatsApp ve Viber gibi VoIP sistemlerinin artan popülaritesi daha düşük fiyata, veri ve ses iletişim hatlarının entegrasyon olasılığına ve gelişmiş PC ve mobil cihaz tabanlı araçların kullanımına dayanmaktadır. YouTube ve benzeri servislerle İnternet, geleneksel multimedya ve eğlence servisleriyle de yakınlaşmaktadır. IPTV ayrıca multimedya servisleri ile IP tabanlı ağlar arasındaki yakınlaşmayı da sağlamaktadır.

Teknik yakınlaşma hızla ilerlerken, ekonomik ve yasal sonuçlarının gelişmesi biraz zaman almaktadır.

Uluslararası düzeyde, yönetim mekanizmaları temel olarak yakınlaşma alanındaki en iyi uygulamaların ve deneyimlerin değişimi için kullanılmaktadır. ITU'nun Telekomünikasyon Geliştirme Sektörü (ITU - D) yaklaşan çevre üzerinde bir çalışma grubuna sahiptir. CoE yaklaşmanın bir yönünü kapsayan medya ve bilgi konusunda geleneksel ve yeni dijital medya arasında aracı rol oynayan bir yönlendirme komitesine sahiptir. Yakınlaşma, net tarafsızlığı, NesNet, araçların rolü, e-ticaret, tüketicinin korunması ve vergilendirme ile doğrudan ilgilidir.

Meseleler

Yakınlaşmanın ekonomik sonuçları

Ekonomik düzeyde yakınlaşma, daha önce ayrı alanlarda faaliyet gösteren şirketleri doğrudan rekabete sokarak geleneksel pazarları yeniden şekillendirmeye başlamıştır. Nihayi olarak, yakınlaşma, iş liderleri arasında “Uber sendromu” korkusuyla sonuçlanmıştır: Tamamen farklı bir iş modeline sahip bir rekabetçinin endüstriye girdiği ve rekabeti düzleştirdiği bir senaryo.⁸⁷ Über, teknolojik açıdan yenilikler yaparak taksi pazarına girdiğinde böyle olmuştur. Sonuç olarak, işletmelerinin tehdit altında olduğunu düşünen geleneksel taksi şirketleri ve sürücüler, pazardaki yeni düzenlemeye girmemiş katılımcıları protesto etmek için dünya genelinde mahkemelere dava açmışlardır.

Şirketler yakınlaşmanın getirdiği zorluklarla baş etmek için farklı stratejiler kullanmaktadır. Sık karşılaşılan bir yaklaşım, piyasadaki OTT sağlayıcılarının daha küçük, daha yeni firmaların daha büyük şirketler ile birleştiği veya bu şirketlerce satın alındığı birleşme ve devralmalar olmuştur. Daha yeni bir yaklaşımda, OTT sağlayıcıları ve telekom sağlayıcıları, her iki tarafa da avantaj sağlayan ortaklıklar kurmaya başlamışlardır. Telekom sağlayıcıları için, OTT sağlayıcılarıyla ortaklıklar, onlara son kullanıcılar için katma değer sağlamanın yanı sıra rekabet avantajı getirebilir. Öte yandan, OTT sağlayıcıları, taşıyıcılarla kurulan ortaklıklar sayesinde hizmetlerinin daha kolay bulunmasını ve erişimlerini sağlamaktadır.⁸⁸

Yakınsayan çevrede düzenleme

Yasal sistem teknolojik ve ekonomik yakınlaşmanın neden olduğu değişikliklere uyum sağlama-daki en yavaş sistemdir. Telekomünikasyon, yayın ve bilgi sunumu gibi her bölüm kendi özel düzenleyici çerçevesine sahiptir. Bu yakınlaşma yönetimle ilgili ve düzenleyici birkaç soruyu gündeme getirmiştir:

- Telefon ve yayıncılık gibi alanlarda mevcut ulusal ve uluslararası düzenlemelere ne olacak?
- Çoğunlukla birleştirilmiş hizmetlere odaklanan yeni düzenleyici rejimlere ihtiyaç var mı? Yoksa, örneğin geleneksel elektronik iletişim servisleriyle aynı düzenleyici çerçevelere mi maruz kalmalılar?
- Rekabet ve tüketicinin korunmasına gelince, yakınsak hizmet sağlayıcılara hangi kurallar uygulanmalıdır?
- Yakınlaşma düzenlemesi kamu makamları (devletler ve uluslararası kuruluşlar) tarafından mı yoksa bağımsız düzenleme yoluyla mı yapılmalıdır?

Ülkeler bu tür soruları çeşitli şekillerde ele almaktadır. AB üyesi ülkeler, Hindistan ve Kenya gibi bazı ülkeler, net IP tarafsızlık ilkeleri bakımından sorunları ele alarak, yakınlaşmayı düzenlemeye yönelik esnek yaklaşımlar seçmişlerdir, çünkü kullanıcıların IP ağları üzerinden sağlanan herhangi bir tür uygulama veya hizmeti seçmelerine izin verilmiştir. Diğer ülkeler, birleştirilmiş hizmetler için yeni yasal veya düzenleyici çerçeveler oluşturmayı seçmişlerdir. Örneğin Kore, IPTV için lisanslama gereklilikleri ve hizmet yükümlülükleri hakkında hükümler içeren özel bir [İnternet Multimedya Yayını İş Yasasına](#) sahiptir. Bazı ülkeler de yakınlaşmanın kendi kendini düzenlemesi yoluyla ele alınmaktadır. Örneğin, Avustralya'da, (iletişim endüstrisindeki çeşitli şirketleri temsil eden İletişim İttifakı, VoIP hizmetleri hakkında birkaç rehber geliştirmiştir.⁸⁹

Bununla birlikte, birleşik hizmetlerin, özellikle VoIP'nin, yasak olduğu veya bir noktada düzenlemelerle açıkça yasaklandığı bazı ülkeler de bulunmaktadır. Örnekler arasında Fas, Belize, Birleşik Arap Emirlikleri de bulunmaktadır.

www.igbook.info/convergence

Son notlar

- 1 İnternet ve www terimleri bazen birbirlerinin yerine kullanılır; Ancak, arada bir fark vardır. İnternet, TCP / IP ile bağlı bir ağ ağıdır. Bazen, İnternet terimi altyapıyı, uygulamaları (e - posta, ftp, Web) ve içeriği kapsamak için kullanılır. Www, HyperText Transfer Protocol'ün (HTTP) yardımı ile birbirine bağlı birleştirilmiş belgeler sistemi olan pek çok İnternet uygulamasından sadece bir tanesidir.
- 2 Bir teknolojik tarafsızlık politikasının ardından AB, “telekomünikasyon” yerine “elektronik iletişim” terimini kullanmaktadır. Bu, örneğin telekomünikasyon altyapısının bir parçası olmayan elektrik şebekesi üzerinden internet trafiğini de kapsar.
- 3 Power Line Communications (PLC), İnternet verilerinin elektrik şebekesi üzerinden iletilmesine izin verir. Derin kılcallığı göz önüne alındığında, elektrik şebekesinin kullanılması, İnterneti birçok kullanıcı için daha erişilebilir hale getirecektir. Bu imkanın teknik ve örgütsel bir incelemesi için, lütfen bkz: Palet J (2003) Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication, Internet Society, ISOC Member Briefing No. 13. <http://www.isoc.org/briefings/013> [Erişim 7 Ekim 2016].
- 4 Project Loon, genişbant kapsamını artırmak ve herhangi bir telekom altyapısına sahip olmayan dünyanın en uzak bölgelerine ulaşmak amacıyla Google tarafından başlatıldı. Şirket, her biri son kullanıcılara bir sinyal veren yüzer bir baz istasyonu olarak hareket eden, yaklaşık 20 km yükseklikte stratosfere çok sayıda balon yerleştirmektedir. Balonlar, ortak telekom operatörleri tarafından sağlanan yüksek hızlı bağlantılar yoluyla birbirine ve yer baz istasyonlarına bağlanmaktadır.
- 5 ITU'ye göre, Televizyon Beyaz Alanları '[TV] yayını tarafından kullanılmayan ve ayrıca yapraklı spektrum olarak da adlandırılan spektrum parçaları' dır. Kullanılmayan frekanslar, UHF [TV] özgü avantajlı yayılma özellikleri sağlayan (mükemmel dış mekan ve iç mekan kapsama alanına sahip ve görünür yayılma özellikleri olmayan hat olan) spektruma ait olduğundan, ITU Radyo Haberleşme Bürosundan Cristian Gomez'in açıkladığı üzere TVWS'nin, kırsal alanlardaki geniş bant uygulamalarına ve NesNet uygulamalarına hizmet edebilen alternatif bir geniş aralıklı düşük güç teknolojisi olarak görülmektedir. Daha fazla bilgi için, lütfen bkz: ITU (2012) Digital Dividend: Insights for Spectrum Decisions. http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf [Erişim 7 Ekim 2016], and Gomez C (2013) TV White Spaces: Managing spaces or better managing inefficiencies? http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR_paper_WhiteSpaces_Gomez.pdf [Erişim 18 Temmuz 2016].
- 6 DTÖ üyelerinin telekomünikasyon piyasalarını serbestleştirilmesi 1998 yılında Temel Telekomünikasyon Anlaşması (BTA) olarak bilinen anlaşmayla resmileştirilmiştir. BTA'nın kabul edilmesinin ardından, 100'den fazla ülke, ulusal telekomünikasyon tekelinin özelleştirilmesi, rekabetin başlatılması ve ulusal düzenleyici otoritelerin kurulması ile karakterize edilen serbestleştirme sürecine başlamıştır. (30 Nisan 1996'da kabul edildi ve 5 Şubat 1998'de yürürlüğe giren) Anlaşma resmen, Hizmet Ticareti Genel Anlaşmasının Dördüncü Protokolü olarak adlandırılmaktadır . http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm [Erişim 7 Ekim 2016].
- 7 ITU (no date) Signatories of the Final Acts – WCIT-12. <http://www.itu.int/osg/wcit-12/highlights/signatories.html> [Erişim 7 Ekim 2016].
- 8 ITU'nun internet ile ilgili faaliyetlerine ilişkin daha fazla bilgi için bkz. <http://www.itu.int/en/action/internet/Pages/default.aspx> [Erişim 7 Ekim 2016].
- 9 Robert Kahn (TCP / IP'nin mucitlerinden biri) tarafından başlatılan bir proje olan Dijital Nesne Mimarisi, her dijital nesneyi (veri ve cihazlar) benzersiz tanımlayıcılar ile ilişkilendirmeyi amaç-

lamaktadır. Bu tür tanımlayıcılar, nesnenin ağlarda nerede bulunduğu, sahip olduğuna, hangi teknolojiye dayandığına bakılmaksızın, değişmeden kalması amaçlanmaktadır. DOA ile ilgili hususları yönetme sorumluluğu, İsviçre merkezli DONA Vakfı'na aittir. ITU, Telekomünikasyon Sektörü çalışma grupları aracılığıyla, DOA'yı bulut bilişim ve NesNet cihazları için bir standart olarak kabul etme olasılığını araştırmaktadır. Bazı ITU üye devletleri DOA standartlarının benimsenmesini savunurken, cihazların sahteciliği ile mücadele gibi nedenleri öne sürerek, cihazların izlenmesine izin vererek, kullanıcı eylemleri kadar DOA'nın da bilgi akışını izlemek ve kontrol etmek için kötüye kullanılabileceğine dair görüşler de bulunmaktadır. Daha fazla bilgi için, bkz: Corporation for National Research Initiatives (2010) A Brief Overview of the Digital Object Architecture and its Application to Identification, Discovery, Resolution and Access to Information in Digital Form. http://www.cnri.reston.va.us/papers/Digital_Object_Architecture_Brief_Overview.pdf [Erişim 20 Ekim 2016]; Javed D (2016) ITU IoT Standards: Gateway to Government Control? <http://www.wileyconnect.com/home/2016/9/20/itu-iot-standards-gateway-to-government-control> [Erişim 20 Ekim 2016].

- 10 DTÖ'nün telekomünikasyon alanındaki rolü ile ilgili daha fazla bilgi için bkz. http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm [Erişim 7 Ekim 2016].
- 11 Bu kısım şuna dayanmaktadır: Kurbalija J (2016) From harmonising cyberpolicies to promoting twi-plomacy: How diplomacy can strengthen Asia-Europe's digital connectivity. In Asia-Europe Foundation. ASEF Outlook Report 2016/2017. Connectivity: Facts and Perspectives, Volume II: Connecting Asia and Europe. <http://www.asef.org/images/docs/ASEF%20Outlook%20Report%202016-2017%20Vol2.pdf> [Erişim 20 Ekim 2016].
- 12 UNESCAP (2014) Problems and Challenges in Transit Connectivity Routes and International Gateways in Asia. Discussion paper series, 2014/1. http://www.unescap.org/sites/default/files/Discussion%20Paper-Transit-Connectivity_0.pdf [Erişim 20 Ekim 2016].
- 13 Verda M (2014) Trans-Eurasian Information Super Highway. <http://sam.az/uploads/PDF/TRANS-EURASIAN%20INFORMATION%20SUPER%20HIGHWAY.pdf> [Erişim 20 Ekim 2016].
- 14 Dijital İpek Yolu terimi, gayri resmi olarak Asya ve Avrupa arasındaki dijital alanda çeşitli işbirliği projelerini kapsayan bir şemsiye kavram olarak kullanılmaktadır. Daha fazla başvuru için, bkz: Jia L and Shuang G (2015) Digital Silk Road to span Eurasia, China Daily Europe, 10 July. http://europe.chinadaily.com.cn/epaper/2015-07/10/content_21241323.htm [Erişim 20 Ekim 2016]; and Zhao Huanxin Z (2015) Web companies asked to support 'digital Silk Road,' China Daily Europe, 8 September. http://www.chinadaily.com.cn/business/2015chinaforum/2015-09/08/content_21823475.htm [Erişim 20 Ekim 2016]. Dijital İpek Yolu, kıtayı geçmesi gereken karasal tabanlı İpek Yolu Ekonomik Kemer ve Çin'i Güneydoğu Asya, Güney Asya, Orta Doğu, Doğu Afrika ve Akdenizdeniz bölgelerine bağlayan Denizcilik İpek Yolu'ndan oluşan Bir Kemer, Bir Yol (yidai - yulu) girişiminin bir parçasıdır. Genel projenin, dünya nüfusunun % 63'ünü oluşturan toplam 4,4 milyar nüfusa sahip 60 ülkeyi geçmesi planlanmaktadır. Daha fazlası için bkz: Arase D (2015) China's Two Silk Roads Initiative: What It Means for Southeast Asia. Southeast Asian Affairs 41, pp. 25–45; and Tsao R (2015) One belt one road: A historical perspective. Chinese American Forum 31(1) pp. 11–14.
- 15 Radyo spektrum politikası hakkında daha fazlası için bkz. <http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy> [Erişim 7 Ekim 2016].
- 16 Bilgisayar ağlarında, değiş-tokuş, her bir ağın müşterileri arasında trafik alışverişi yapmak amacıyla idari olarak ayrı internet ağlarının gönüllü bir bağlantısıdır. Tam tanımı, ücretsiz ya da 'gönderen herkesi açık' şeklindedir; yani, hiç kimse paylaşılan trafik için diğerine ödeme yapmaz; bunun yerine,

her biri kendi müşterilerinden gelir elde eder. Eşleme, ağların fiziksel olarak birbirine bağlanması ve Sınır Ağ Geçidi Protokolü (BGP) yönlendirme protokolü aracılığıyla bir yönlendirme bilgisi alışverişini gerektirir. Bu sıklıkla, el sıkışmaktan kesin sözleşmelere kadar çeşitli formalitelere sahip anlaşmalarla yapılmaktadır. (Kaynak: Wiki- pedia).

- 17 Katman 2 İnternet Bant genişliği Sağlayıcıları genellikle ICP (internet bağlantı noktaları) veya internet geçitleri olarak adlandırılırlar.
- 18 İki ilgili durumdan şu kaynakta söz edilmektedir: Spaink K (2002) Freedom of the Internet, our new challenge. http://www.spaink.net/english/osce_internetfreedom.html [Erişim 7 Ekim 2016]. İlk durumda, Flashback'in İsveç'te barındırdığı şüpheli Nazi içerikli bir web sayfasına karşı yasal işlem başlatıldı. Mahkemeler, sayfanın İsveç'li Nazi karşıtı yasalarını ihlal etmediğine karar verdi. Bununla birlikte, bir Nazi karşıtı eylemci, Flashback'e karşı güçlü bir kampanya başlattı ve böylece Flashback'in ISS'e, Air2Net'e ve ana omurga operatörü MCI / WorldCom'a baskı uyguladı. Bu kampanyanın baskısı altında, MCI / WorldCom, bunu yapmak için yasal dayanak olmamasına rağmen Flashback'in bağlantısını kesmeye karar verdi. Flashback'in alternatif bir sağlayıcı bulma girişimleri başarısız oldu, çünkü bunların çoğu MCI / WorldCom tarafından işletilen omurgayla da bağlandı. İkinci dava Hollanda'da gerçekleşti. Hollandalı küçük bir ISS sağlayıcısı Xtended Internet, Scientology lobisinin baskısı altındaki ABD merkezli yukarı akış sağlayıcısı ile bağlantısı kesildi.
- 19 Metz C (2016) Facebook and Microsoft are laying a giant cable across the Atlantic. Wired, 26 May. <http://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/> [Erişim 7 Ekim 2016].
- 20 IANA kendisini İnternet'in en eski Kurumlarından biri olarak nitelendirmektedir. Bu kurumun işlevleri işlerin sadece bir kişi (o sırada Güney Kaliforniya Üniversitesi ile çalışan bir bilgisayar bilimcisi olan Jon Postel) tarafından gerçekleştirildiği 1970'lere kadar geriye gider. 1998'den başlayarak, IANA işlevleri ABD hükümeti ile yapılan bir sözleşmeye dayanarak ICANN tarafından gerçekleştirilmiştir. Bu sözleşmenin sona ermesinin ardından 1 Ekim 2016'da, yeni kurulan bir ICANN iştiraki olan PTI tarafından gerçekleştirilmeye devam edilmiştir. IANA işlevleri üç kategoride gruplandırılabilir: etki alanı adları (DNS kökünün yönetimi, .int ve .arpa alanları ve bir IDN uygulamaları kaynağı), sayı kaynakları (öncelikle IP ve Özerk sayılar havuzunun koordinasyonu; bunları RIR'lere) ve protokol atamaları (İnternet protokolünün numaralandırma sistemlerinin yönetimi standart kurumlarla birlikte yapılır). Daha fazla bilgi için bkz. <https://www.iana.org/about> [Erişim 7 Ekim 2016].
- 21 Mevcut RIRler: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean Network Information Centre), RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East) and AFRINIC (the African Network Information Centre). RIR sisteminin detaylı bir açıklaması için bkz. <http://www.ripe.net/internet-coordination/internet-governance/internet-technical-community/the-rir-system> [Erişim 7 Ekim 2016].
- 22 Drake W et al., Internet Fragmentation: An Overview. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [Erişim 7 Ekim 2016].
- 23 Örneğin, 2000 yılında, IETF IPv6 düğümlerinin İnternet'te IPv6 dağıtımını büyük ölçüde kolaylaştıracak IPv4 ile tam uyumluluğunu sürdürmesini sağlayacak geçiş mekanizmalarını tanımlayan IPv6 ve İnternetin sonunda IPv6'ya geçişini kolaylaştıracak olan Sunucuları ve Yönlendiricileri için Geçiş Mekanizmaları RFC 2893'ü hazırladı. <https://www.ietf.org/rfc/rfc2893.txt> [Erişim 7 Ekim 2016].
- 24 8 Haziran 2011'de gerçekleştirilen başarılı bir Dünya IPv6 Günü etkinliğinin ardından, dünyadaki belli başlı ISS'ler, ev ağı ekipmanı üreticileri ve web şirketleri, IPv6'yı 6 Haziran 2012 tarihine kadar ürün ve hizmetleri için kalıcı olarak sağlamak üzere bir araya geldi - Dünya IPv6'nın lansmanı. 2016

- yılında, Dünya IPv6'nın başlamasından dört yıl sonra, küresel IPv6 trafiğinin% 500'den fazla büyüdüğü bildirildi. Daha fazla detay için bkz. <http://www.worldipv6launch.org> [Erişim 7 Ekim 2016].
- 25 Daha kapsamlı ve teknik TCP/IP Güvenliği için bkz. http://www.linuxsecurity.com/resource_files/documentation/tcpip-securi-ty.html [Erişim 7 Ekim 2016].
 - 26 Bavisi J (2011) What Security Issues does IPv6 Pose? eSecurity Planet. <http://www.esecurityplanet.com/trends/article.php/3935356/What-Security-Issues-Does-IPv6-Pose.htm> [Erişim 25 Temmuz 2016].
 - 27 Ashford W (2011) IPv6: The security risks to business. Computer Weekly, 29 Ağustos. <http://www.computerweekly.com/feature/IPv6-The-security-risks-to-business> [Erişim 26 Temmuz 2016].
 - 28 Grup hakkında daha detaylı bilgi için bkz. <http://www.etsi.org/technologies-clusters/technologies/next-generation-protocols> [Erişim 7 Ekim 2016].
 - 29 DNS'in yönetim yapısını belirleyen birkaç doküman için bkz. RFC 1591 (March 1994), which specifies the governance structure of DNS. <http://www.ietf.org/rfc/rfc1591.txt> [Erişim 7 Ekim 2016].
 - 30 ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. <https://www.icann.org/resources/pages/governance/bylaws-en> [Erişim 7 Ekim 2016].
 - 31 Kütük Anlaşmalarının bir listesi için bkz. <https://www.icann.org/resources/pages/registries/registries-agreements-en> [Erişim 7 Ekim 2016].
 - 32 Alan adı tescilli hizmetlerini gTLD'ler altında, gTLD kayıt defterlerine doğrudan erişimle sağlamak isteyen kayıt sahiplerinin ICANN tarafından onaylanması gerekir. Bu tür kayıt (kütük) tutucuların bir listesi için bkz. <https://www.icann.org/registrar-reports/accredited-list.html> [Erişim 7 Ekim 2016].
 - 33 Delege edilmiş dizinleri içeren yeni gTLDler hakkındaki istatistikler için bkz. <https://www.icann.org/en/program-status/statistics> [Erişim 7 Ekim 2016].
 - 34 The IANA Report on the county code top-level domain for Palestine <http://www.iana.org/reports/ps-report-22mar00.htm> [Erişim 7 Ekim 2016].
 - 35 ccTLDler için kütükler hakkındaki detaylar için bkz. IANA Root Zone Database <http://www.iana.org/domains/root/db> [Erişim 7 Ekim 2016].
 - 36 Ülke etki alanlarının yönetimine ilişkin Brezilya modeli genellikle çok paydaşlı yaklaşımın başarılı bir örneği olarak belirtilir. Brezilya etki alanlarından sorumlu ulusal kurum, devlet yetkilileri, iş sektörü ve sivil toplum dahil olmak üzere tüm kilit oyunculara açıktır. Daha fazla bilgi için bkz: Alfonso C (2004) BR: CCTLD An asset of the commons, in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 291–299; Excerpts <http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false> [Erişim 14 Ekim 2016].
 - 37 Örneğin, Güney Afrika, egemen haklarını, ülke alanının kontrolünü geri kazanmada bir argüman olarak kullandı. Ülke etki alanının Güney Afrika hükümeti tarafından belirlenen parametrelerin dışında kullanılmasının suç sayılacağını belirten bir yasa kabul edildi. Kamboçya'nın ülke etki alanı yönetimini hükümet dışından devlet kontrolüne devretmesi genellikle başarısız bir geçiş örneği olarak gösteriliyor. Hükümet, hizmet kalitesini düşürdü ve Kamboçyalı alan adlarının kaydını çok daha zor hale getiren daha yüksek ücretler getirdi. Daha fazla bilgi için bkz. Klien N (2004) Internet Governance: Perspectives from Cambodia in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 227–237. <http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false> [Erişim 7 Ekim 2016].

- 38 Bir ccTLD'nin yetkilendirilmesi ve yeniden yetkilendirilmesi hakkında daha fazla bilgi için, ülke kodlu üst düzey bir alanın (ccTLD) Delegasyonu veya yeniden dağıtılması ile ilgili IANA kılavuzuna bkz. <http://www.iana.org/help/ccld-delegation> [Erişim 7 Ekim 2016].
- 39 ICANN GAC (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains. https://gacweb.icann.org/display/GACADV/ccTLDs?previ ew=/28278844/28475457/ccTLD_Principles_0.pdf [Erişim 14 Ekim 2016].
- 40 Kök bölge dosyası için bkz. <http://www.iana.org/domains/root/files> [Erişim 7 Ekim 2016].
- 41 Kök bölge sunucuları, düğümleri ve pozisyonlarının ve yöneten organizasyonların listesi için bkz. <http://www.root-servers.org/> [Erişim 7 Ekim 2016].
- 42 DNS kök bölgesindeki 13 yetkilinin listesi için bkz. <http://www.iana.org/domains/root/servers> [Erişim 9 Ekim 2016].
- 43 ISC Inc. (2003) Hierarchical Anycast for Global Distribution. <http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.html> [Erişim 14 Ekim 2016].
- 44 Daha fazla detay için bkz. Das D (2015) List of top 4 alternative DNS servers to your ISP. <http://www.snaphow.com/4402/list-of-top-4-alternative-dns-servers-to-your-isp/> [Erişim 7 Ekim 2016].
- 45 Yeti DNS Projesi hakkında daha fazla detay için bkz. <https://yeti-dns.org> [Erişim 7 Ekim 2016].
- 46 Alternatif kök sistemleri ile ilgili zorluklar hakkında daha kapsamlı bir analiz için bkz. Bertola V (no date) Oversight and multiple root server systems. http://wgig.org/docs/book/Vittorio_Bertola.html [Erişim 7 Ekim 2016].
- 47 Sinyal iletim teknolojileri - hem kablosuz, hem Uzun Vadeli Evrim (LTE), hem de Yoğun Dalga Boyu Bölmeli Çoklama (DWDM) gibi optik kablolar için - "bant genişliği tükenmesi" sorununu çok daha fazla bant genişliği spesifikasyonu (saniyede terabit kadar) çözme vaat etmektedir. Bununla birlikte, talep-arz koşuşturması devam etmektedir.
- 48 The Economist (2009) America insists on net neutrality: The rights of bits. 24 September. <http://www.economist.com/node/14517422> [Erişim 7 Ekim 2016].
- 49 Verizon ve Google'ın Açık İnternet Yasal Çerçeve Önerisinin tam metni için bkz. http://www.google.com/googlegbgs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf [Erişim 7 Ekim 2016].
- 50 ISS ile yapılan bir sözleşmede kabul edilen bant genişliği (bit hızı) aslında, garantili bir efektif hızdan ziyade sadece maksimum olanıdır.
- 51 McCullagh D (2012) European ISPs defend UN Internet tax. C|net, 20 Ağustos. http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defend-u-n-internet-tax/ [Erişim 7 Ekim 2016].
- 52 Halen tartışmalı olan ve gelecekte görüşülecek olan unsurlar köşeli parantez içindedir.
- 53 Radunović V (2012) Network neutrality in law – a step forwards or a step backwards? Diplo Blog. <http://www.diplomacy.edu/blog/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards> [Erişim 14 Ekim 2016].
- 54 Federal Communications Commission (2015) Open Internet Order. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [Erişim 8 Ağustos 2016].
- 55 Dava, Amerika Birleşik Devletleri Columbia Bölgesi Devresi Temyiz Mahkemesi tarafından ele alındı ve Mahkeme kararı için bkz. [https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/\\$file/15-1063-1619173.pdf](https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf) [Erişim 14 Ekim 2016].
- 56 European Union (2015) Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 Kasım 2015 laying down measures concerning open internet access and amending Directive

- 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) 531/2012 on roaming on public mobile communications networks within the Union. <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R2120> [Erişim 8 Ağustos 2016].
- 57 BEREC, Haziran 2016'da, yeni net tarafsızlık kurallarının ulusal düzenleyici otoriteler tarafından nasıl uygulanacağına ilişkin bir taslak kılavuz taslağı yayınladığında, büyük Avrupalı telekomünikasyon sağlayıcıları, önerilen kılavuzların '5G'nin yatırım getirisi ile ilgili önemli belirsizlikler yaratacağını savunarak tepki verdiler. '5G'nin ortak bir platformda, ölçekte ve hizmet garantileriyle geniş bir yelpazede çeşitli endüstri iş modellerine izin vermeyi amaçlayan "ağ dilimleme" kavramını getirdiğini açıkladı. Onlara göre, teklif "aşırı derecede kuralcıdır ve telekomünikasyon şirketlerinin riskini olumsuz yönde etkileyebilir, böylece 5G ağ dilimlemenin son kullanıcı / uygulama ve trafik taleplerindeki değişikliklere gerçek zamanlı uyum sağlamanın temel çevikliğini ve esnek doğasını göz ardı ederek 5G sömürüsünü engelleyebilir. Avrupa Yayın Birliği gibi diğer kuruluşlar, sağlam ağ tarafsızlığı kurallarının "açık ve birlikte çalışabilen 5G teknoloji platformunun" geliştirilmesi için anahtar olacağını düşünerek bu görüşe katılmamaktadır. Daha fazla ayrıntı için, Patterson G ve ark. (2016) Avrupa'da 5G'nin zamanında konuşlandırılması için Manifesto. Daha fazlası için bkz. Patterson G et al. (2016) Manifesto for timely deployment of 5G in Europe. <http://telecoms.com/wp-content/blogs.dir/1/files/2016/07/5GManifestofortimelydeploymentof5GinEurope.pdf> [ac- cessed 9 Ağustos 2016]; and European Broadcasting Union (2016) EBU response to the public consultation of draft BEREC guidelines on implementation of net neutrality rules. http://www.ebu.ch/files/live/sites/ebu/files/Publications/Position%20Papers/EBU_response_BEREC_consultation_NN_guidelines_final_version_18072016.pdf [Erişim 9 Ağustos 2016].
- 58 Body of European Regulators for Electronic Communications (2016) Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules [Erişim 7 Ekim 2016].
- 59 Brazilian Marco Civil'in İngilizce versiyonu için bkz. <http://www.giplatform.org/resources/text-brazilsnew-marco-civil> [Erişim 8 Ekim 2016].
- 60 TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. <http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of> [Erişim 8 Ekim 2016].
- 61 European Digital Rights (2013) Slovenia has a net neutrality law. <https://edri.org/edriagramnumber11-2slovenia-net-neutrality/> [Erişim 8 Ağustos 2016].
- 62 Electronic Frontier Foundation (2012) The Netherlands passes net neutrality legislation. <https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation> [Erişim 8 Ağustos 2016].
- 63 Norwegian Communications Authority (2009) Guidelines for Internet neutrality. http://eng.nkom.no/technical/internet/net-neutrality/net-neutrality/_attachment/9222?ts=1409aa375c1 [Erişim 7 Ekim 2016].
- 64 The integral text of the 2010 Declaration of the Committee of Ministers on network neutrality is <https://wcd.coe.int/ViewDoc.jsp?id=1678287> [Erişim 9 Ağustos 2016]. 2016 Bakanlar Komitesi'nin ifade özgürlüğü ve tarafsızlığa ilişkin mahremiyet haklarının korunması ve teşvik edilmesi konusundaki önerisi için bkz. [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2016\)1&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)1&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true) [Erişim 9 Ağustos 2016].

- 65 Internet Society (no date) Net Neutrality. <http://www.internetsociety.org/net-neutrality> [Erişim 3 Kasım 2016].
- 66 TACD (2015) Resolution on the open and neutral Internet. <http://tacd.org/wp-content/uploads/2015/06/TACD-Infosoc-Resolution-on-Net-Neutrality-2015-Green.pdf> [Erişim 3 Kasım 2016].
- 67 Global Multistakeholder Meeting on the Future of Internet Governance (2014) NETmundial Multistakeholder Statement. <http://netmundial.br/netmundial-multistakeholder-statement/> [Erişim 14 Ekim 2016].
- 68 Radunović V (2012) Can free choice hurt open Internet markets? Diplo Blog. <http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets> [Erişim 7 Ekim 2016].
- 69 International Telecommunication Union (2016) ITU towards 'IMT for 2020 and beyond'. Available at <http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx> [Erişim 7 Ekim 2016].
- 70 Güncel İnternet standartları, taslak standartlar ve önerilen standartların güncellenmiş listeleri Resmi İnternet Protokol Standartları dizininde bulunmaktadır. <https://www.rfc-editor.org/standards> [Erişim 7 Ekim 2016].
- 71 World Wide Web Consortium (no date) Standards. <http://www.w3.org/standards/> [Erişim 14 Ekim 2016].
- 72 Gecikme, bir veri paketinin bir ağ içinde belirtilen bir noktadan diğerine ulaşması için geçen süre anlamına gelir.
- 73 Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [Erişim 7 Ekim 2016].
- 74 Oracle (2016) Oracle Unveils Suite of Breakthrough Services to Help Simplify Cloud Adoption by Global Corporation. <https://www.oracle.com/corporate/pressrelease/oracle-cloud-at-customer-032416.html> [Erişim 7 Ekim 2016].
- 75 The Open Group (2013) Cloud Computing Portability and Interoperability. http://www.opengroup.org/cloud/cloud_iop/ [Erişim 7 Ekim 2016].
- 76 IDC (2014). The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. <http://www.emc.com/leadership/digital-universe/2014view/digital-universe-of-opportunities-vernon-turner.htm> [Erişim 7 Ekim 2016].
- 77 Verizon (2016) State of the Market: Internet of Things 2016. <http://www.verizon.com/about/our-company/state-of-the-market-internet-of-things> [Erişim 7 Ekim 2016].
- 78 IITU and Cisco Systems (2016) Harnessing the Internet of Things for Global Development. <http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf> [Erişim 7 Ekim 2016].
- 79 Schmid S et al. (2016) EnLighting: An Indoor Visible Light Communication System Based on Networked Lights Bulbs. <https://s3-us-west-1.amazonaws.com/disneyresearch/wp-content/uploads/20160615205959/EnLighting-An-Indoor-Visible-Light-Communication-System-based-on-Networked-Light-Bulbs-Paper.pdf> [Erişim 7 Ekim 2016].
- 80 Hollanda'da, ülke çapında IoT çözümleri (LoRa) için özel bir ağ Temmuz 2016'da Hollandalı bir telekom şirketi olan KPN tarafından konuşlandırıldı. Güney Kore'de, Samsung ve SK Telecom, ülke genelinde ticari bir IoT'ye özel ağın kullanıma açılması üzerine çalışıyor.

- 81 Eylül-Ekim 2016'da, birçok IoT cihazından faydalanan iki büyük DDoS saldırısı, büyük web sitelerinin erişilmesini engelledi. ABD güvenlik araştırmacısına ve Fransız bir şebeke servis sağlayıcısına yapılan saldırılarda bir milyondan fazla cihaz kullanıldı. İkinci saldırı, bir günde üç saldırı geçiren DNS servis sağlayıcısı Dyn tarafından işletilen sistemlere yönelikti; Saldırıları Twitter, PayPal, Netflix, Airbnb, Amazon, CNN ve birkaç çevrimiçi dergiyi etkiledi. Detaylar için bkz. Rash W (2016) Weak Devices security turns IoT into powerful weapon in DDos attacks. Eweek, 1 Ekim. <http://www.eweek.com/security/weak-device-security-turns-iot-into-powerful-weapon-in-ddos-attacks.html> [Erişim 12 Kasım 2016]. Wikipedia (2016) 2016 Dyn cyberattack. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack [Erişim 12 Kasım 2016].
- 82 Greenberg A (2016) Inside Google's Internet Justice League and its AI-powered war on trolls. Wired, 19 September. <https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/> [Erişim 20 Ekim 2016].
- 83 Romm T (2016) Tech companies launch new AI coalition. Politico, 11 Ekim. <http://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600> [Erişim 20 Ekim 2016].
- 84 European Parliament Committee on Legal Affairs (2016) Draft report with recommendations to the Commission on Civil Law Rules on Robotics. [http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2015/2103\(INL\)&cl=en](http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2015/2103(INL)&cl=en) [Erişim 7 Ekim 2016].
- 85 US National Science and Technology Council (2016) The National Artificial Intelligence Research and Development Strategic Plan. https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf [Erişim 20 Ekim 2016].
- 86 UK Parliamentary Committee on Science and technology (2016) Robotics and artificial intelligence. <http://www.publications.parliament.uk/pa/cm201617/cmselect/cm-scitech/145/14502.htm> [Erişim 20 Ekim 2016].
- 87 IBM Institute for Business Value (2016) Redefining Boundaries. Insights from the Global C-suite Study. <https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03695usen/GBE03695USEN.PDF> [Erişim 7 Ekim 2016].
- 88 Telekomünikasyon sağlayıcıları ve OTT sağlayıcıları arasındaki ortaklıklar hakkında daha fazla bilgi için bkz. Body of European Regulator for Electronic Communications (2016) Report on OTT services. <http://www.stibbe.com/-/media/03%20news/newsletters/brussels/bru%20tmt%20bereg%20report%20on%20ott%20services.pdf> [Erişim 7 Ekim 2016].
- 89 For more details on the various legal and regulatory approaches towards convergence, read: ITU, infoDev (no date) Impact of Convergence. <http://www.ictregulationtoolkit.org/6.4> [Erişim 7 Ekim 2016].

The background is a solid teal color. It features several large, semi-transparent geometric shapes: a large inverted triangle at the top left, a smaller inverted triangle at the top right, a circle with diagonal lines on the right side, and several large triangles at the bottom, some of which are semi-transparent and overlap each other.

Bölüm 3

Güvenlik Sepeti

GÜVENLİK SEPETİ

Siber güvenlik

İnternet esasında başta akademisyenler olmak üzere kapalı bir çevre tarafından kullanılmak üzere tasarlanmıştı. İletişim açıldı. Güvenlik endişe edilecek bir husus değildi.

Siber güvenlik, İnternet'in öncülerin döngüsünün ötesine geçmesiyle daha önemli hale geldi. İnternet, teknolojinin hem kolaylaştırıcı hem de tehdit edici olabileceği gerçeğini bir kez daha ortaya getirmiştir. Toplumun avantajına kullanılan şey dezavantajına da kullanılabilir.

3 milyardan fazla kullanıcısı olan modern internet, günümüz toplumunun kritik altyapısıdır (CI). İnternetin güvenlik açığı, modern toplumun güvenlik açığıdır. Mali sektör, devlet hizmetleri, güvenlik sektörü, okullar, hastaneler ve vatandaşlar giderek daha fazla ve geri dönüşü olmayan bir şekilde birbirine ve küresel ağa bağlı hale gelmektedir.

Ayrıca, ülkeler arasındaki siyasi gerilimler siber alana yansımakta, bazen siber hadiseleri tetiklemektedir. Siber hadiseler, özellikle CI ile ilgili olanlar, devletin çalışması, ekonomi ve refah bakımından korkunç sonuçlar doğurabilir. Örneğin, İsviçre'ye yapılan ülke ölçeğinde bir siber saldırı, günde doğrudan 500 milyon Euro'nun üzerinde bir kayıpla sonuçlanabilir.¹

Siber güvenliğin haritalandırılması

Siber güvenlik meseleleri üç kritere göre sınıflandırılabilir:

- **Eylem türü.** Eylem türüne göre sınıflandırma, veri durdurma, veri etkileşimi, yasadışı erişim, casus yazılım, veri bozulması, sabotaj, hizmet dışı bırakma (DoS) ve kimlik hırsızlığını içerebilir.
- **Fail türü.** Muhtemel failer arasında suçlular, anarşistler, bilgisayar korsanları, devrimciler, teröristler, gizli servisler, savunma ve askeri birimler bulunabilir.
- **Hedef türü.** Bireylerden, özel şirketlerden, sivil toplum kuruluşlarından, medya kuruluşlarından ve kamu kurumlarından çekirdek İnternet altyapısına (telekom işletmecileri, ISP'ler, IXP'ler, veri merkezleri), kritik toplum altyapısına (elektrik ve su, sanayi tesisleri, trafik vb.) ve askeri varlıklara kadar potansiyel hedefler çok çeşitlidir.

Siber güvenlik çerçevesi, siber güvenlik ile ilgili politika ilkelerini, araçlarını ve kurumlarını içerir. Siber güvenlik, çeşitli alanları kapsayan bir şemsiye kavramdır:

- **Kritik bilgi altyapısının korunması** (CIIP) giderek daha önemli hale gelmektedir, çünkü enerji, su, iletişim ve finans dahil CI'ların artık bilgi altyapısının altında yatan İnternet ve diğer bilgisayar ağlarına bağlıdır. Kritik bilgi altyapısı (CII) sadece (güvenlikleri genel olarak ağ güvenliği olarak anılan) donanıma ve bağlantıları değil, ayrıca protokolleri, veri merkezlerini ve kritik İnternet kaynaklarını da içermektedir.
- **Siber suç**, internet ve bilgisayar sistemleri aracılığıyla işlenen bir suçtur. Siber suç, eski,

yani, (çeşitli dolandırıcılıklar gibi) siber alanda gerçekleştirilen geleneksel suçları, (kredi kartı sahtekarlığı ve çevrimiçi çocuk istismarı ve sömürüsü gibi) teknolojiye bağlı suçları, (DoS saldırıları ve tıklama başına ödeme sahtekarlıkları gibi) İnternet ile ortaya çıkan yeni suçları ve genellikle karanlık piyasalar yoluyla yayılan (virüsler ve botnetler gibi) siber suç araçlarının ticarileştirilmesi gibi suçları kapsamaktadır. **Çevrimiçi çocuk cinsel istismarı ve sömürüsüyle** mücadele, siber suçlara karşı uluslararası işbirliği alanında en gelişmiş alandır. **İnternet güvenliği** olarak adlandırılan tüm kullanıcıların ve özellikle çocukların güvenliğinin çoğunlukla eğitim ve bilinçlendirme yoluyla arttırılması, suçun, dolandırıcılıkların veya zorbalığın önlenmesi için önemli bir adımdır.

- Genellikle siber savaş olarak etiketlenen **siber çatışmalar**, yüksek medya görünürlüğüne sahiptir, ancak politika ve yasal açıdan daha az dikkat çekmektedir. Siber çatışmalarla ilgili işbirliği üç ana alana ayrılır: siber çatışmaların (esasen **Lahey Sözleşmeleri** olmak üzere mevcut yasalar siber alana uygulanabilir olup olmadığı; yoksa, ne tür yeni yasal araçlar geliştirilmesi gerektiği şeklinde) yönetilmesi; silahlar ve silahsızlanma (yani, siber silahların silahsızlanma sürecine nasıl sokulacağı); ve insancıl hukuk (yani, Cenevre Sözleşmelerinin siber çatışmalara nasıl uygulanacağı). **Ekonomik temelli siber casusluk**, siyasi belgelerin sızdırılmasını sağlayan hackler ve savaş eylemleri eşliğinde sabotaj davranışı, politik ve diplomatik gündemlerin en üst sırasında yer almaktadır. İnternetin giderek **teröristler tarafından** bilgi, iletişim, propaganda ve bazen de siber terörizm olarak adlandırılan saldırılar için **kullanılması**, kovuşturulması bazen ulusal ceza hukukuna göre yapılmasına rağmen, siyasi olarak ulusal ve küresel güvenlik meselesi olarak anılmaktadır.

Siber güvenlik tehditleri

Güvenlik tehditlerine çeşitli failler ve çeşitli motifler sebep olabilir. Bireylere saldırırken, failler genellikle onların para veya mal varlığını ele geçirmek için bilgiye ve kişisel verilere erişmeye çalışırlar. Virüs veya casus yazılım, kimlik avı ve e-dolandırıcılık gibi kötü amaçlı yazılımlar, internet kullanıcıları için en yaygın tehditlerdir. Ayrıca, casusluk amacıyla karmaşık şirket ve hükümet sistemlerine nüfuz etmek için daha karmaşık saldırılar gerçekleştirilmektedir. Benzer şekilde, tüm üç taraflı sistemi veya ağı bozmak için çeşitli siber silahlar ve saldırılar bir arada kullanılabilir.

Veri ve sistemlerin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyen saldırı türlerini kolaylaştırmak için kullanılan teknikler çok çeşitli ve oldukça sofistikedir.

Kötücül yazılım (malware), virüs, casus yazılım ve dijital cihazlara izinsiz yüklenen ve genellikle saldırganın yararına olmak üzere istenmeyen görevler gerçekleştiren diğer istenmeyen yazılımları içerir. Bu programlar, cihazlara zarar verebilir ve kişisel bilgileri çalmak, çevrimiçi etkinliği izlemek ve kontrol etmek, spam göndermek ve sahtekarlık yapmak ve ayrıca ağdaki diğer cihazlara bulaşmak için kullanılabilir. Ayrıca, istenmeyen veya uygunsuz çevrimiçi reklamlar da yayınlayabilirler.

Virüsler, Truva atları, adware ve casus yazılımların tümü kötü amaçlı yazılım türleridir. Bir virüs, kullanıcının farkında olmadan kendini kopyalayabilir ve diğer cihazlara bulaştırabilir.

Bazı virüsler gizli olmasına rağmen, çoğunun verilerle etkileşime girmesi veya aygıtların performansını etkilemesi (sabit diski yeniden biçimlendirme, bilgisayar belleği kullanma gibi) söz konusudur. Bir Truva atı, faillerin bir cihaza sızmak ve ek uzak işlemleri yürütmek için kullanabilecekleri bir arka kapıya izin vermek için kullanılan kötü amaçlı veya zararlı içerik içeren bir programdır. Truva atları, bir kullanıcının sistemine erişmeye çalışan siber hırsızlar ve bilgisayar korsanları tarafından kullanılabilir. Kullanıcı genellikle bir tür sosyal mühendislik tarafından sistemlerine Truva atlarını yüklemek ve uygulamak için kandırılır. Bir kez etkinleştirildiğinde, Truva atları siber suçluların kullanıcıları gözetlemelerini, hassas verileri çalmalarını ve sistemlerine arka kapı erişimi elde etmelerini sağlayabilir.

Adware, pazarlama bilgisi ve diğer bilgileri kullanıcının bilgisi olmadan toplar veya arama isteklerini belirli reklam web sitelerine yönlendirir. Casus yazılım kullanıcıları izler, onlar hakkında bilgi toplar ve kullanıcı farkında olmadan ilgilenen taraflara iletir. Toplanan bilgi türleri, ziyaret edilen web sitelerini, tarayıcı ve sistem bilgilerini, bilgisayarın IP adresini ve e-posta adresleri ve şifreleri gibi daha hassas bilgileri içerebilir. Ayrıca, kötü amaçlı yazılım, kullanıcının tarayıcı ayarlarının izinsiz olarak değiştirildiği tarayıcı korsanlığına neden olabilir. Yazılım, masaüstü kısayolları oluşturabilir, reklam açılır pencerelerini görüntüleyebilir, mevcut giriş sayfalarını değiştirebilir veya sayfaları başka sayfalarla arayabilir.

Botnetler, sahiplerinin bilgisi olmadan ele geçirilmiş uzaktan kumanda edilen görevleri gerçekleştiren cihazların ağıdır. Bir cihaz, uzaktan kumandaya izin veren belirli bir kötü amaçlı yazılım türünden etkilendikten sonra bir bot'a dönüştürülür. Bot ağı çok çeşitli suçlar ve saldırılar için kullanılır: spam dağıtmak, kötü amaçlı yazılım bulaşmasını daha fazla cihaza yaymak, tıklama başına dolandırıcılık ödemelerine veya kimlik hırsızlığına katkıda bulunmak gibi. Botnet'lerin en endişe verici kullanımlarından biri, dağıtılmış hizmet reddi (DDoS) saldırıları gerçekleştirmektir (Şekil 11).



Şekil 11. Botnet

Araştırmacılar ve siber güvenlik şirketleri, botnetlerin, virüslerin ve diğer kötü amaçlı programların etkilerini artırdığı, bilgi hırsızlığı yarattığı ve DoS saldırılarını artırdığı için, İnternet güvenliği tehdidi haline geldikleri konusunda uyarı yapmaktadır. Bu tehdit boyutunun bir örneği olarak Nisan 2015'te indirilen Simda botnet, 190 ülkede bilgisayarları etkilemiş ve 5 ülkede 14 komuta ve kontrol sunucusunun kullanımına sirayet etmiştir.²

DoS saldırıları, bir bilgisayarın veya web sitesinin bilgi talepleriyle dolmasına yol açar ve düzgün çalışmasını engeller. Bu saldırılar, kullanıcıların bunlara erişmesini önlemek için bir ağ, uygulama veya hizmet için mevcut kaynakları tüketmeyi amaçlar. Bireylerden ziyade işletmeler daha sık hedeftedir. **DDoS** saldırıları, birden fazla ele geçirilmiş bilgisayarın tek bir hedefe saldırdığı saldırılardır.

Bir DoS saldırısı genellikle bilgi hırsızlığına veya diğer güvenlik kayıplarına yol açmaz, ancak etkilerinden dolayı etkilenen kuruluş veya birey bakımından (belirli ağ hizmetleri kullanılamıyor hale gelmesi, web sitelerinin çalışmaması, e. posta hesaplarının e-postaları almamaları, vb gibi nedenlerle) mali kayıplara veya zaman kaybına neden olabilir

Kimlik Avı, bir kişinin normalde yapmaması gereken bir şeyi yapması için kandırıldığı, (kullanıcı adı ve şifre gibi) gizli bilgiler sağlama, bilinmeyen bir dosya açma veya güvenilir olmayan bir bağlantıyı takip etme gibi bir sosyal mühendislik şeklidir. Bir kimlik avı biçimi, e-posta,

sosyal medya veya diğer çevrimiçi hizmetlerden, alıcının kişisel veya hassas bilgiler sağlaması için (banka gibi) mevcut ve güvenilir bir varlık olduğunu iddia etmekten ibarettir.

E-dolandırıcılık, dolandırıcıların potansiyel mağdurlarla iletişim kurmak için (genellikle iş veya yatırım fırsatları, kolay para kazanma yolları, sağlık veya çevrimiçi alışverişlerde önemli indirimler gibi) çeşitli konularda e-posta veya web siteleri gibi çevrimiçi yolları kullanmasıdır. E-dolandırıcılık, e-posta sahtekarlığı ve gittikçe artan şekilde sosyal medya ile ilişkilendirilmektedir.

Siber güvenlik politikası ve düzenlemeler

Birçok ulusal, bölgesel ve küresel girişim, siber güvenliğe odaklanır. Ulusal düzeyde, artan mevzuat ve içtihat hacminin, siber suçla mücadele ve gittikçe artan bir şekilde, CII'nin terörizm veya çatışmaların bir sonucu olarak sabotaj ve saldırılara karşı korunmasına odaklanması siber güvenlik ile ilişkilidir. Siber güvenliğe odaklanmayan gelişmiş bir ülke bulmak zordur. Bölgesel ve küresel düzeyde de birçok girişim ve faaliyet mevcuttur.

Küresel siber güvenlik faaliyetleri

Birleşmiş Milletler

BM, bir süredir siber güvenlik konusunu tartışmaktadır. 1998 yılında, Rusya Federasyonu, UNGA'nın İlk Komitesinde bilgi güvenliği ve telekomünikasyon alanındaki gelişmeler hakkında bilgi güvenliği bağlamında bir karar taslağı sunmuştur.³ Daha sonra 2004 yılında, BM siber alandaki mevcut ve potansiyel tehditlerin ve bunlara yönelik olası işbirlikçi önlemlerin incelenmesi amacıyla GGE kurulmuştur. Grubun görevi 2009, 2011, 2013 ve 2015 yıllarında yeniden teyit edilmiştir. BM GGE 2013 raporunun ana sonucu, mevcut uluslararası hukukun devletler tarafından BİT kullanımı için geçerli olduğu ilkesinin teyidi olmuştur. Ayrıca, 2015 raporu bir devletin, CI'nın kullanımına ve işleyişine zarar verecek veya başka şekilde zarar verecek olan BİT faaliyetlerini yürütmemesi veya bilerek desteklememesi gerektiğini de belirtmektedir.⁴

Birleşmiş Milletler Silahsızlanma Konferansı, siber güvenliğin yüksek diplomatik düzeyde tartışılması için başka bir olanak sunmaktadır. Şimdiye kadar, Çin gibi bazı üyeler, siber güvenliğin gündeme eklenmesini önermiş olsa da, grup bir çalışma planı üzerinde anlaşamamıştır.⁵

Siber suç alanında, Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) önde gelen bir kuruluştur. **Birleşmiş Milletler Organize Organize Suçlara Karşı BM Sözleşmesi** (UNTOC) gibi UNODC'nin yasal araçlarından bazıları siber suçla mücadelede kullanılmaktadır. Siber suçların çoğu (en az üç kişi tarafından) organize edilir ve (birden fazla devlette örgütlenmiş ve hatta bir devlette gruplar tarafından organize edilen) sınır ötesi suçlardır.

Uluslararası Telekomünikasyon Birliği

ITU, 2005 yılında, Tunus Gündemi'nin C5 Eylem Çizgisi'nin BİT Kullanımında Güven ve Güvenlik Oluşturma başlıklı Eylem Planı'nı takip etmesi için WSIS sonuçları tarafından görevlendirilmiştir.

ITU, siber güvenlik ile ilgili birçok faaliyet yürütmektedir. Bununla birlikte, telekomünikasyon altyapısının güvenliği ile ilgili bu çalışmaların yalnızca bir kısmı karar verme (ya da daha doğrusu standart ayar) niteliğindedir; bunların çoğu araştırma, farkındalık ve kapasite geliştirmeyi içerir.

En göze çarpan faaliyetlerden biri, ITU Genel Sekreteri tarafından, bilgi toplumunda güven ve güvenliği arttırmayı amaçlayan uluslararası işbirliğinin bir çerçevesi olarak 2007’de başlatılan ITU **Küresel Siber Güvenlik Gündemidir** (GCA).⁶ GCA, işbirliği ve verimlilik için, ilgili tüm ortaklarla birlikte ve arasında işbirliğini teşvik etmek ve mevcut girişimleri tekrarlı çabaları önlemek üzere tasarlanmıştır. ITU, Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklığı (IMPACT) ile ülkelere dünya çapında siber güvenlik çözümleri ve politikaları oluşturmalarına yardımcı olmaktadır. GCA beş stratejik sütun üzerine kuruludur: yasal önlemler, teknik ve prosedürel önlemler, organizasyon yapıları, kapasite geliştirme ve uluslararası işbirliği.

Bir diğer ITU etkinliği, ülkelerin siber güvenliğe olan bağlılığını ölçmeyi amaçlayan çok paydaşlı bir girişim olan **Küresel Siber Güvenlik Endeksidir** (GCI).⁷

İnternet Yönetişimi Forumu

Siber güvenlik, IGF’nin 2006’daki ilk toplantısından bu yana IGF’in gündeminde öne çıkmıştır. Örneğin, Siber güvenlik Kasım 2015’te Brezilya’daki João Pessoa’daki IGF toplantısında güvenlik, şifreleme ve güven odaklı ana oturumların ve birkaç atölye oturumunun konularından birisiydi.⁸ IGF 2015’teki atölye çalışmalarının beşte biri siber güvenlikle ilgili konuları ele almıştır. 2016 yılında, siber güvenlik, IGF’in siber güvenlik alanındaki paydaş grupları arasındaki ortaklığa ve işbirliğine odaklı En İyi Uygulama Forumunun konusu olarak seçilmiştir. IGF kararlar vermez veya tavsiyelerde bulunmazken, her yıl düzenlenen En İyi Uygulama Forumları ve tematik oturumları yoluyla açık diyalog ve ortaklık, bilgi alışverişi ve faydalı gönüllü politikalar için fırsat yaratmaktadır.

Siber Uzay Küresel Konferansı

Siber Uzay Küresel Konferansı (GCCS), ‘siber uzayda yöneten davranış’ ile ilgili ilkeleri tartışan bir dizi konferans olarak ortaya çıkmıştır.⁹ Konferanslar ilk konferansın 2011’de Londra’da yapılmasından bu yana bazen Londra Süreci olarak da adlandırılır. İkinci konferans 2012’de Budapeşte’de, üçüncüsü 2013’te Seul’de ve dördüncüsü 2015’te Lahey’de yapılmıştır.

GCCS, birçok bakan da dahil olmak üzere hükümet temsilcilerinin yanı sıra kurumsal sektör ve sivil toplumun üst düzey temsilcilerini bir araya getirmektedir. Başkanın Beyanı dışında herhangi bir sonuç veya resmi uzlaşma üretmemekte, ancak diğer çerçevede gelecekteki olası uzlaşmalar hususunda müzakere platformu da dahil tartışmalar ve işbirliği için de önemli fırsatlar sağlamaktadır.

GCSC 2015’te, siber kapasite oluşturma konusundaki deneyimlerin paylaşılması, boşlukların belirlenmesi ve mevcut çabaların tamamlanması amacıyla Küresel Siber Uzmanlık Forumu

(GFCE) kurulmuştur. Forum üyeleri teknik topluluk, sivil toplum örgütleri ve akademi ile birlikte siber kapasite geliştirme alanında inisiyatifler geliştirmek için birlikte çalışan hükümetler, uluslararası kuruluşlar ve özel şirketlerdir. Tüm üyeler daha fazla kapasite geliştirme, en iyi uygulamaların paylaşılması ve uluslararası işbirliğinin güçlendirilmesi ihtiyacını vurgulayan [Lahey Deklarasyonu](#)'nu kabul etmiştir.¹⁰

NATO

Kolektif bir savunma örgütü olan NATO, siber güvenlikle ilgili olarak siber savunma konusundaki çabalara odaklanmaktadır. NATO, teknolojiye ve İnternete olan bağımlılığın artmasıyla ortaya çıkan tehdit ortamındaki hızlı değişiklikleri takip etmiş ve siber savunmayı stratejik ve kurumsal çerçevesine sıkıca yerleştirmiştir. Örgütün doktrin çerçevesinde bile değişiklikler olmuştur. 28 üye devlet 2016'da siber alanı hava, kara ve denizin yanı sıra dördüncü operasyonel alan olarak ilan edilmesi konusunda anlaşmıştır.¹¹

2014 yılında kabul edilen mevcut [NATO'nun Siber Savunma Politikası](#), diğer konuların yanı sıra, üye devletlere farkındalık, eğitim, eğitim ve egzersiz etkinliklerinin yürütülmesi için yol gösteren ve sektörün dışında diğer uluslararası kurumlar olmak üzere ortaklarla daha ileri işbirliği girişimlerinin sürdürülmesi ihtiyacını vurgulayan prosedürler içermektedir. NATO'nun siber savunmada en büyük önceliği, kuruluşun sahip olduğu ve işlettiği iletişim ve bilgi sistemlerinin korunması olmasına rağmen, üye devletlerinin de güvenilir ve güvenli bir ulusal altyapıya sahip olmasına vurgu yapmaktadır.

NATO öncülüğünde kurulan Kooperatif Siber Savunma Mükemmeliyet Merkezi'ni (CCD COE), araştırmacı ve uygulamacı yönelimli eğitim programlarından oluşan 'uluslararası siber hukuk araştırmaları ve eğitiminde öncü bir çaba olarak' siber alana uygulanan uluslararası hukuka ilişkin öneriler içeren temel bir uluslararası doküman olarak [Siber Savaşta Uygulanabilir Uluslararası Hukuk Tallinn Elkitabı](#) adı altında 2009'da Tallinn Elkitabı Sürecini devreye sokmuştur.¹² CCD COE ayrıca, kamu politikası formülasyonun farklı düzeylerine göre ulusal siber güvenliğin muhtelif yönlerini anlamaya yardımcı olacak ayrıntılı bilgi ve derinlemesine teorik çerçeve sağlayan bir [Ulusal Siber Güvenlik Çerçeve Kılavuzu](#) da geliştirmiştir. Her biri ulusal siber güvenlik konusunda kendi bakış açılarına sahip ve herbiri El Kitabı içerisinde kendi bölümleri olan siyasi, stratejik, operasyonel ve taktik/teknik yönetim konusu bulunmaktadır. Ayrıca, El Kitabı, ulusal siber güvenlik alanında, üst düzey politika koordinasyon organlarından siber kriz yönetimi yapılarına ve benzeri kurumlara kadar ilgili kurumlara örnekler vermektedir.¹³

Bölgesel siber güvenlik faaliyetleri

Bölgesel düzeyde, gittikçe daha fazla sayıda kuruluş siber güvenliğin önemini fark etmekte ve [CoE Siber Suçlar Sözleşmesi](#), [Asya-Pasifik Ekonomik İşbirliği \(APEC\) Güvenli Çevrimiçi Alan Stratejisi](#), [AB Siber Güvenlik Stratejisi](#), [OSCE'nin Güven Artırıcı Önlemler Konusundaki Konvansiyon Kararı](#) ve [Afrika Siber Güvenlik Sözleşmesi](#) gibi stratejiler, tavsiyeler ve sözleşmeler üzerinde çalışmaktadır.

Avrupa

Avrupa, siber güvenliği ele alan ilk bölgelerden biriydi. CoE, 1 Temmuz 2004'te yürürlüğe giren **Siber Suçlar Sözleşmesini**¹⁴ kabul etti. Sözleşme, dünya çapında siber suçlarla ilgili birçok bölgesel ve ulusal düzenlemeye ilham vermiştir. Avrupa, ABD, Kanada, Japonya ve Avrupa dışındaki diğer bazı ülkeler tarafından onaylanan sözleşme dijital alanda hala önemli bir uluslararası yasal araçtır. Birkaç Avrupa üyesi olmayan ülke tarafından onaylandığı göz önüne alındığında, Sözleşmeyi küresel bir siber suç aracı olarak ele alma hakkında tartışmalar ortaya çıkmıştır. Bununla birlikte, bazı ülkeler (aracın müzakeresine katılmamak gibi) sembolik olanlardan (örneğin sınır ötesi soruşturmaların ortaya çıkma olasılığı gibi) önemli olanlara kadar farklı nedenlerden dolayı Sözleşme rezerv koymuştur.

AB düzeyinde, **Siber Güvenlik Stratejisi** ve **ağ ve bilgi sistemlerinin güvenliği ile ilgili Yönerge** (NIS Yönergesi), siber güvenlik alanındaki iki ana belgedir. Strateji, AB için siber esnekliği sağlamaya, siber suç süresini önemli ölçüde azaltmaya, siber savunma politikası ve yetenekleri geliştirmeye, siber güvenlik için endüstriyel ve teknolojik kaynakları geliştirmeye, uyumlu bir uluslararası siber güvenlik politikası oluşturmaya ve tutarlı bir yapı kurmaya odaklanarak, siber alandaki güvenlik sorunlarının ele alınmasına yönelik bir dizi stratejik öncelik ve eylemin ana hatlarını çizmektedir.¹⁵ Yönerge, AB içerisinde yüksek düzeyde ortak bir siber güvenliğin sağlanması amacıyla üye devletler tarafından uygulanacak önlemler hakkında hükümler içermektedir. Bu önlemler arasında, diğerlerinin yanı sıra, ağ ve bilgi sistemlerinin güvenliği konusunda ulusal stratejilerin benimsenmesi, ulusal yetkili makamların ve Bilgisayar Güvenliği Olay Müdahale Ekiplerinin (CSIRT'ler) belirlenmesi ve uygun güvenlik önlemlerini almayı empoze edecek özellikli hizmetlerin işletmecilerinin belirlenmesi yer almaktadır.¹⁶

OSCE ayrıca siber güvenlik ve özellikle güven artırıcı önlemlerin (CBM'ler) geliştirilmesi konusunda da çalışmaktadır. Bu önlemler genellikle devletler arasındaki ilişkilerin iyileştirilmesine, bir çatışmanın barışçıl bir şekilde çözüme kavuşturulmasına veya askeri çatışmaların patlak vermesinin önlenmesine yardımcı olmak için tasarlanmıştır. OSCE Daimi Konseyinin CBM'ler konusundaki iki kararı, OSCE'nin siber alana katılımının en dikkat çekici örnekleridir. 2013'ten itibaren ilk OSCE CBM seti, ICT kullanımından kaynaklanan çatışma risklerini azaltmayı amaçlamaktadır.¹⁷ Bu gönüllü önlemler, tehditler ve en iyi uygulamalar hakkında ulusal görüşlerin paylaşılmasını, yetkili ulusal kurumlarla işbirliği yapmayı, yanlış algılamayı ve olası gerginliği veya uyuşmazlık risklerini azaltma konusunda danışmanlık yapmayı, bilgi paylaşımına olanak sağlamak için ulusal yasalar oluşturmaya ve siber güvenlikle ilgili ulusal terminolojiyi paylaşmayı ve tartışmayı içermektedir. 2016 yılında, ikinci CBM grubu, özellikle kamusal özel ortaklıklar (PPP'ler) konusunda kapsamını genişletmiştir.¹⁸

Yakın gelecekte OSCE içerisinde yeni CBM kümelerinin kararlaştırılması beklenmektedir. Daha da önemlisi, CBM'lerin başarısı diplomatik topluluklara nüfuz ettiğinden, CBM'lerin de BM GGE'nin daha fazla çalışmasını desteklemesi muhtemeldir.

Amerika

2003'te Amerikan Devletleri Örgütü (OAS), Amerikan Terörizmle Mücadele Komitesi (CIC-TE), Adalet Bakanları veya Diğer Bakanlar, Amerikan Devletleri Başsavcıları (REMJA) ve Ame-

rikan Devletleri Arası Telekomünikasyon Komisyonu (CITEL) olmak üzere örgütün üç ilgili grubunun çabalarını bir araya getiren [Amerikan Devletler Arası Siber Güvenlik Stratejisini](#)¹⁹ oluşturmuştur. Bu gruplar, siber suçları önleyecek ve CI'yı yasal ve diğer usule ilişkin tedbirlerle koruyacak programları uygulamak için üye devletlerle birlikte çalışmaktadır. REMJA'nın bir parçası olan Siber Suçlar Çalışma Grubu, üye devletlerin siber suç ve elektronik kanıtlarla ilgili yasal düzenlemeler ve prosedürel tedbirler geliştirme kapasitelerini güçlendirmek için teknik atölye çalışmaları düzenlemektedir.²⁰

Asya

Asya'da, Güneydoğu Asya Ülkeleri Birliği (ASEAN) Bölgesel Forumu (ARF) siber güvenlik güven artırıcı önlemler ve siber suçlarla mücadele konusunu ele almaktadır. 2012 yılında ARF, ICT güvenliği konusunda bölgesel işbirliğini yoğunlaştırmayı amaçlayan bir bakanlık raporu hazırlamıştır.²¹ 2013 yılında Ulusötesi Suçla İlgili Kıdemli Yetkililer Toplantısı Siber Suçla ilgili Çalışma Grubu kurmaya karar vermişken, ARF, terör ve ulus ötesi suçla mücadeleye odaklanarak siber güvenliği tekrar gündeminde almıştır.²²

Çin, Rusya ve Orta Asya ülkelerini içeren Şangay İşbirliği Örgütü'nün (SCO) siber güvenlik alanında çok yoğun faaliyetleri bulunmaktadır. Uluslararası bilgi güvenliğini sağlama alanındaki işbirliği konusunda bir anlaşma yapılmıştır. Dahası, 2011'in sonunda, SCO üyeleri, BM'ye 2015 yılında güncellenerek yeniden sunulan bir Bilgi Güvenliği için Uluslararası Davranış Kuralları önerisi sunmuştur.²³

Afrika

Afrika'da, siber güvenlik politikası, [Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesinin](#)²⁴ hazırlanmasına odaklanmıştır. Bu sözleşme şu anda onay sürecindedir. Genel olarak, Afrika'da asıl odak nokta, siber güvenlik ile ilgili ulusal ve bölgesel kuruluşlar için kapasite geliştirme üzerinedir.

İkili faaliyetler

Giderek artan bir şekilde, ülkeler siber güvenlik konularını ele almak için ikili yollar kullanmaktadır. Bunlar koordinasyon anlaşmaları yoluyla ikili anlaşmalardan gayri resmi istişarelere kadar uzanmaktadır. ABD, siber suç konularında işbirliği yapmak için 20'den fazla ülke tarafından imzalanan Karşılıklı Adli Yardım Anlaşmaları'nı (MLAT) kullanmaktadır. Birçok ülke, bilgi alışverişini ve koordineli faaliyetleri belirten siber güvenlik işbirliği anlaşmaları imzalamıştır.

Ayrıca, büyük siber güvenlik aktörleri işbirliğini artırmanın ve olası çatışmayı engellemenin bir yolu olarak düzenli ikili diyalogları kullanmaktadır. Örneğin, Çin'in hem ABD hem de AB ile diyalogu bulunmaktadır. Avustralya, Çin, ABD, Güney Kore, Hindistan ve Yeni Zelanda ile siber diyaloglar geliştirmiştir. Hindistan ve Rusya bir siber güvenlik diyalogu kurmuşlar ve 2016'da resmi bir siber anlaşma imzalamışlardır.

Teknik ve akademik inisiyatifler

CERT'ler/CSIRT'ler siber güvenlik alanındaki teknik işbirliğinin ana aracı olmuştur. CERT'ler bölgesel işbirliği yoluyla ulusal sınırlar boyunca işbirliği yapmaktadır. Olay Yeri Müdahale ve Güvenlik Ekipleri Forumu (FIRST), ulusal CERT'lerin uluslararası teknik ağını koordine etmektedir.

İş dünyasının inisiyatifleri

Güvenliği artırmak için gittikçe artan sayıda girişim iş dünyasından, özellikle de en büyük yazılım ve donanım üreticilerinden gelmektedir. İş dünyasının genel uluslararası politika çerçevesine dahil olması, bir yandan düzenleyici olanlarla birlikte teknolojik iyileştirmeler getirme ihtiyacı, bir yandan da son kullanıcılar tarafından teknolojiye olan güven ve güveni artırma konusundaki kendi çıkarları ile motive edilmektedir.

Microsoft, genel olarak diplomatlar ve devletlerin alanı olan uluslararası barış alanında kurumsal bir oyuncunun ilk girişimi olan siber alandaki²⁵ çatışmayı azaltma yönünde bir dizi siber güvenlik normu önermiştir. Microsoft, Uluslararası Yüksek Teknoloji Suç Soruşturma Birliği (HTCIA) ile işbirliği içinde, siber suç soruşturmalarına yardımcı olmak için kolluk kuvvetleri tarafından erişilebilecek bir Dijital Suçlar Topluluğu Portalı başlatmıştır.

Cisco, BT uzmanları ve organizasyonları için bir dizi ağ güvenliği sertifikası geliştirmiştir.

Microsoft, SAP, Cisco ve diğerleri de dahil olmak üzere tüm dünyadaki çeşitli çok uluslu yazılım ve donanım şirketlerinde yer alan araştırma ve üniversite ilişkileri departmanları teknolojik yenilikleri teşvik etmek için araştırma, öğrenim ve öğretim tecrübesini geliştirmek için önde gelen üniversiteler, devlet kurumları, meslek kuruluşları ve endüstri ortakları ile güçlü ilişkiler kurmaya odaklanmıştır. İşbirliği, yerel akademik kurumlar ve bu şirketlerin yerel araştırma birimleri arasında ortak araştırma çalışmaları, araştırma hibeleri, konferans desteği, doktora çalışmaları için burslar veya üniversiteler, kurumlar ve okullarla yapılan diğer yenilikçi müfredatı yaymaya yönelik çeşitli programlar aracılığıyla gerçekleştirilmiştir.

Siber güvenlik meselelerinde temel zorluklar

Siber güvenlikte terminolojik karmaşa

İnternet kamu politikası bir politika alanıdır. Bu nedenle, (siber/e/dijital/net/ sanal gibi) ön eklerin birbirinin yerine kullanımı gibi iyi niyetli kullanımlardan temel farklılıklara kadar farklı terimlerin kullanımının farklı politikaları yansıttığı birçok terminolojik karışıklık söz konusudur. Siber güvenlik alanında, bu politika alanını tanımlamak için kullanılan yaygın isimden başlayarak karışıklık potansiyeli önemlidir. Çin, Rusya ve SCO ülkeleri, politik ve sosyal istikrarı da kapsayan daha geniş bilgi güvenliği terimini kullanmaktadır. Siber güvenliği, bilgi güvenliğinin teknik bir alt kümesi olarak görmektedirler. ABD, AB ve OECD ülkeleri için siber güvenlik, temel olarak İnternet altyapısının korunmasına odaklanan bir şemsiye terimdir. Bu ülkeler için bilgi güvenliği, esas olarak veri ve bilgi ile uğraşan bir siber güvenliğin alt kümesidir.

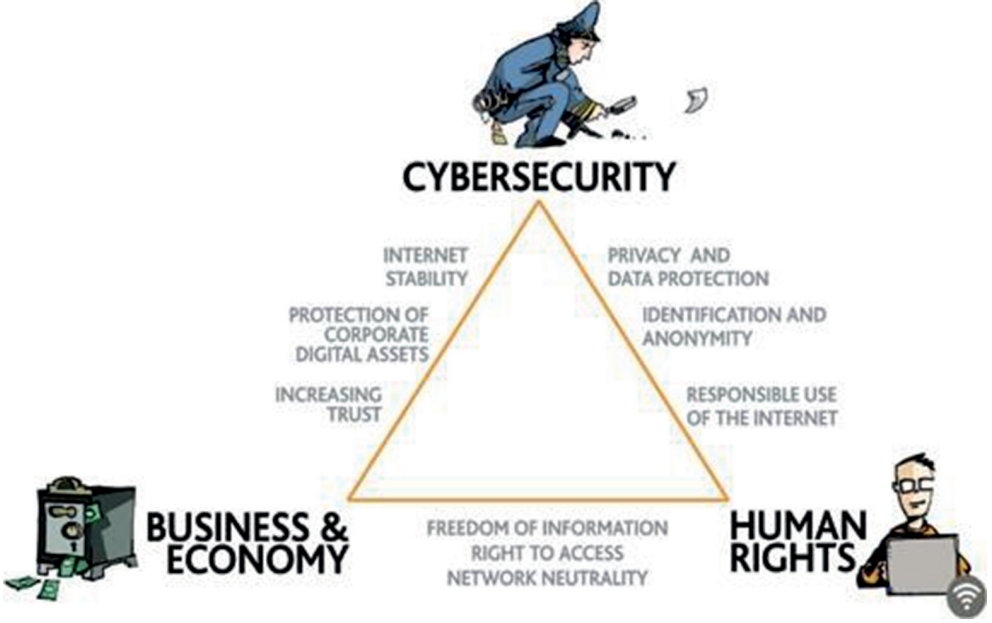
Çeşitli oyuncuların CII, siber silahlar ve siber terör gibi kavramları anlama şekillerinde de farklılıklar vardır. Bu terminolojik karışıklığa değinmek çok önemlidir. Siber güvenlik konusunda ortak bir anlayışa ulaşmak için uluslararası toplumun çok fazla zamana ve uzun süreli müzakerelere ihtiyacı olacaktır. Ne yazık ki, yanlış anlaşılmalara nedeniyle ortaya çıkan riskler acildir ve hafife alınmamalıdır. İlk adım, farklı terminolojileri tanımlamak ve bunların kesin anlamsal kapsamlarını belirlemek olabilir. Farklılıkları belirlemek için bu ilk adımdan sonra, olası yakınlaşmaları tanımlamak ve yavaş yavaş siber güvenlik konusunda ortak bir kelime hazinesi geliştirmek mümkün olabilmelidir.

Siber güvenliğe çok disiplinli yaklaşım

Siber güvenlik, Şekil 12'deki politika üçgeni ile gösterildiği gibi, insan hakları ve ekonomik gelişme gibi dijital politikanın diğer yönlerinden ayrı ele alınamaz.²⁶

Bu nedenle siber güvenlik risklerine anlamlı bir sistematik cevap siber alanın eknoloji, hukuk, psikoloji, sosyoloji, ekonomi, siyaset bilimi ve diplomasi bağıntısı gibi çok disiplinli yönlerinin derinlemesine anlaşılmasına bağlıdır. Cevabın etkinliği ayrıca, risklerin azaltılmasına katkıda bulunabilecek şu paydaşlar arasındaki ortaklıklara dayanmaktadır:

- Siber güvenlik için yasal, düzenleyici ve politika ortamı yaratma yetenekleriyle hükümet ve düzenleyici otoriteler.
- Cezai kovuşturma ve sınır ötesi işbirliği mekanizmalarının yetki ve sorumlulukları ile adli kurumlar ve kanun uygulayıcı makamlar.
- Uzmanlıkları ve fiili olarak altyapı, hizmet ve standartların çoğunluğu üzerindeki kontrolü ile özel sektör ve teknik topluluklar.
- Ağları ve son kullanıcılara ulaşma ve siber alanın kötüye kullanılması konusunda uyarma kapasiteleriyle STK'lar ve akademi dünyası.



Şekil 12. Siber güvenlik politikaları üçgeni

İnternet Teknik mimarisi ve siber güvenlik

İnternetin doğası ve nasıl organize edildiği internet güvenliğini etkiler. Güvenliği halihazırdaki önceden var olan, güvenli olmayan temel üzerine mi inşa etmeliyiz yoksa İnternet altyapısının temelini mi değiştirmeliyiz? Bu tür değişiklikler İnternetin diğer özelliklerini, özellikle açıklığını ve şeffaflığını nasıl etkiler? Geçmişte İnternet standartlarının geliştirilmesi, performansın iyileştirilmesini veya yeni uygulamaların kullanılmasını amaçlıyordu. Güvenlik bir öncelik değildi. IETF'in uygun kimlik doğrulama sağlamak için e-posta standartlarını değiştirip değiştiremeyeceği ve nihayetinde (spam, siber suçlar gibi) İnternet'in kötüye kullanımını azaltıp azaltmayacağı belli değildir.

Temel İnternet standartlarındaki değişiklikleri çevreleyen tartışmalar göz önüne alındığında, temel İnternet protokolündeki güvenlikle ilgili iyileştirmelerin kademeli ve yavaş olması muhtemeldir. Ancak bu yönde önemli adımlar atılmaya başlanmıştır. **Alanı Adı Sistem Güvenlik Uzantıları** (DNSSEC)²⁷ açıklayıcı iyi bir örnektir. Teknik topluluk içindeki yaklaşık 12 yıllık araştırma, deneme ve tartışmaların ardından DNSSEC ilk olarak bazı ccTLD'ler için dağıtılmış ve 2010'dan itibaren kök sunucu düzeyinde de uygulanmıştır. Ancak, bu yeni güvenlik standardının geniş ölçekli uygulanması alan adı kayıt şirketleri, ISS'ler ve web sitesi sahipleri tarafından benimsenmesiyle ilgili başka zorluklar yaşanmaktadır.

Bununla birlikte, güvenlikteki önemli iyileştirmeler, dünyadaki DNS sunucuları gibi ana İnternet düğümlerinin uygun şekilde yapılandırılmasıyla sağlanabilir. 2013 yılında küresel İnternet'in büyük bölümlerinin geçici olarak tıkanmasına neden olan CyberBunker ve Spamhaus şirketleri arasındaki özel siber savaşı gibi birçok olay, dünya çapında [açık alan adı çözümleyicileri](#)²⁸ olarak bilinen birkaç düzine yanlış yapılandırılmış DNS sunucusundan kaynaklanmaktadır. Ayrıca, [tasarım güvenliğini](#) tümüyle yazılım, donanım ve protokoller gibi tüm yeni teknolojilere uygulamak, güçlendirme ve engellemeleri içerebilecek ek güvenlik katmanları getirecektir.

Siber güvenlik, güven, ve e-ticaret

Siber güvenlik, e-ticaretin hızlı büyümesinin ön koşullarından birisi olarak sıkça dile getirilmektedir. Güvenli ve güvenilir bir İnternet olmadan, güven azalacak ve İnternet kullanıcıları, kredi kartı numaraları gibi çevrimiçi gizli bilgileri sağlama konusunda isteksiz olacaklardır. Aynı şekilde çevrimiçi bankacılık ve elektronik para kullanımı için de geçerlidir. 2014 yılında Rusya'daki bir grup tarafından müşterilerin kişisel verilerini ve kredi kartı numaralarını elde etmek için şirketlerin sunucularından, 1.2 milyardan fazla kullanıcı adı ve şifre ve yarım milyar adet e-posta adresinin çalındığı başarılı saldırılara tanık olmaktadır.²⁹ Bu olaylar, çevrimiçi hizmetlerde kullanıcının güvenliğini baltalamaktadır. Eğer sadece genel siber güvenlik (ve beraberindeki standartların yokluğu) yavaş iyileşirse, iş dünyasının siber güvenlik alanında daha hızlı gelişmeleri zorlaması muhtemeldir. Bu, ağ tarafsızlığı ilkesinde ve başka şeylerin yanı sıra, daha güvenli İnternet iletişimini kolaylaştıracak “yeni bir İnternet”in geliştirilmesinde başka zorluklara da yol açabilir.

Gözetim ve casusluk

NSA çalışanı Edward Snowden'in 2013 yılında ifşa ettikleri, ABD'nin de dahil olduğu devletlerin İnternet'in kendi çıkarları için internetin kırılganlıklarından yararlandığını doğrulamıştır. NSA'nın Kişisel Kayıt Bilgi Sistemi Metodolojisi (PRISM) projesi, gözetim kabiliyetlerini, (ABD merkezli telekom, servis ve içerik sağlayıcıları gibi) başlıca İnternet şirketlerinin kablolarına, yönlendiricilerine ve bulut sunucularına erişme yeteneğine dayandırmıştır. Buna cevaben, diğer ülkeler, özellikle AB ve BRICS (Brezilya, Rusya, Hindistan, Çin ve Güney Afrika) kendi kıtalararası denizaltı kablo bağlantılarının³⁰ döşenmesi de dahil olmak üzere bulut sunucularını azaltma taktiklerini dikkate almaya ve İnternet şirketlerinin vatandaşların kişisel verilerini kendi yetki alanları dahilindeki veri merkezlerinde saklamalarını istemeye başlamıştır.

Ekonomik siber casusluk

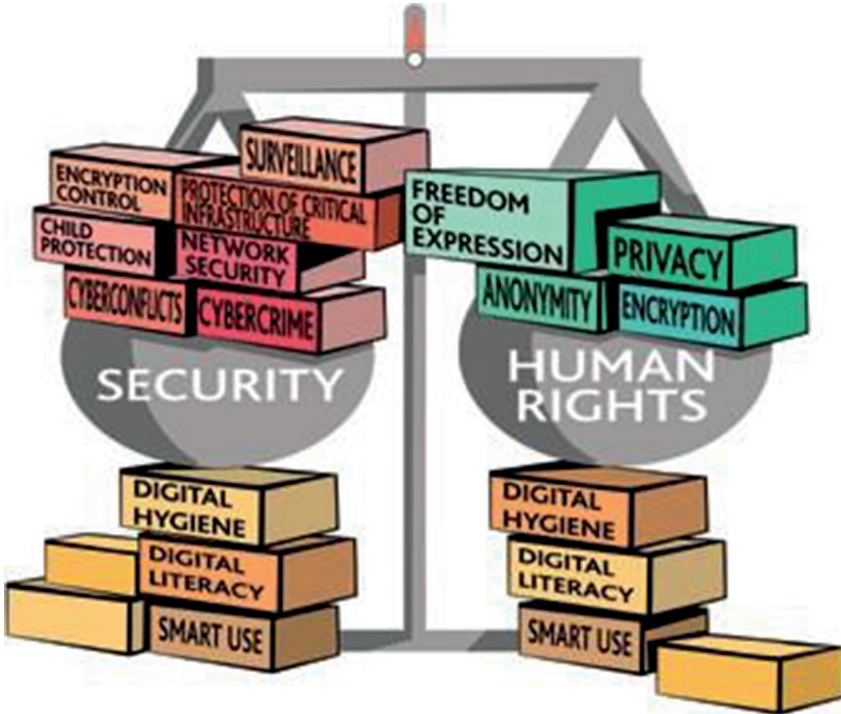
2013 yılında ABD merkezli güvenlik şirketi Mandiant, Çin kaynaklı ABD şirketlerine yönelik siber casusluk saldırıları hakkında bir rapor yayınlamıştır.³¹ ABD beş Çin askeri korsanını suçladıktan sonra Çin, ABD'yi siber casuslukla suçlamış ve bu da Çin'in ABD Siber Çalışma Grubu'nun faaliyetlerinin askıya alınmasına yol açmıştır.³² ABD hükümeti ekonomik siber casusluk nedeniyle Çin'i yaptırımlarla tehdit etmesiyle, Eylül 2015'te Çin Devlet Başkanı Xi Jinping'in

ABD ziyareti öncesinde bu kriz zirveye ulaşmıştır. Ziyaret sırasında iki ülke bilişim şirketlerine karşı siber casusluğu bilerek desteklememeyi kabul etmiştir.³³ Ekonomik siber casusluğa karşı yapılan anlaşma, 15-16 Kasım 2015'te Antalya'daki G20 toplantısında G20 ülkelerinin 'hiç bir ülkenin şirketlere veya ticari sektöre rekabet avantajı kazandırmak maksadıyla ticari sırlar veya gizli işletme bilgileri de dahil fikri mülkiyet haklarının çalınmasını kolaylaştıracak ICT faaliyeti için de bulunmaması veya bu tür faaliyetleri desteklememesi gerektiği' konusunda uzlaşmasıyla ayrıca onay almıştır.³⁴

İstisnalar ve devletlerin hackleme araçlarıyla siber alanın giderek militarizasyonu, artan siyasi gerginliğe yol açmaktadır. Bu gerginlik siber silahların çoğalmasını önlemek için küresel çabalara olan ihtiyacı hızlandırabilir.

Cybersecurity and human rights

Siber güvenlik ve insan hakları arasındaki bağlantı, İnternet'in geleceği için oldukça önemlidir. Şimdiye kadar, bu iki alan kendi silolarında ayrı ayrı ele alınmıştır. Bununla birlikte, son deneyimler (SOPA, ACTA, PRISM / NSA) (mahremiyet, ifade özgürlüğü, erişim gibi) insan haklarının korunmasının yalnızca değere dayalı bir öncelik olmadığını, aynı zamanda İnternet'in açık ve güvenli kalmasını sağlamanın da pratik bir aracı olduğunu göstermektedir.



Şekil 13. Güvenlik ve insan hakları arasında denge kurma

Bireysel İternet kullanıcıları siber güvenliğin temel direkleridir. Yine de, siber saldırılara karşı koruma söz konusu olduğunda, genellikle en zayıf halkadır. Kişisel bilgisayarlarımız (botnet'lerin bir parçası olarak), siber saldırıları düzenlemek, virüs ve kötü amaçlı yazılım yaymak için kullanılır. Bilgisayarlarımıza ve mobil cihazlarımıza korumasız erişim, şirketlerimizin veya kurumlarımızın veri kümelerine erişim için arka kapı sunar ve daha birçok bilgisayarı tehlikeye sokar.

Bununla birlikte, son kullanıcıların endişeleri, genellikle, (sıklıkla cehalet nedeniyle) tehlikeye attıkları bilgisayarların bir sonucu olarak daha büyük hasar ile ilgili değil, genel olarak kendi verilerinin korunması, bütünlüğü ve mahremiyetiyle ilgilidir. Post-PRISM tartışmaları, kişisel bilgisayarları şifreleme, düzenli yamalar ve güncellemeler, IPSec ve VPN'lerin³⁵ nasıl kullanılacağı da dahil olmak üzere 'gözetim-güvenli' hale getirmeyi vurgu yapmaktadır. Bunların farkında olmak, korunmasız erişimi önler ve genel siber güvenliğe katkıda bulunur.

Bireysel İternet kullanıcılarının önemli rolü etrafında şekillenen küresel siber güvenlik, temel taşlarından biri olarak insan haklarını esas alır. Bu bağlantının tanınması politika belgelerinde de ortaya çıkmaya başlamıştır. Örneğin, AB'nin [Siber Güvenlik Stratejisi](#), temel hakların tesisi ve korunması için destek de dahil olmak üzere açık, özgür ve güvenli bir siber alanı korumayı, beş strateji sütunundan biri olarak görmektedir.

Siber güvenlik ve mahremiyet, Şekil 13'te görüldüğü gibi, birbirlerini dengede tutarken tasvir edilir. Bu her zaman böyle değildir.

Asıl zorluk, kazan/kazan çözümlerini hedeflemektir. Daha fazla güvenlik, daha fazla insan hakları anlamına gelir veya bunun tersi de geçerlidir. Aslında, öncelik verilmesi gereken siber güvenlik sisteminin payandaları olarak (bilgiye erişim, mahremiyet koruması gibi konularda) bireylerin güçlendirilmesi ve korunması noktasında birçok kazan/kazan alanı vardır. Sonuçta, insan hakları siber güvenliğin realpolitik meselesidir.

www.igbook.info/cybersecurity

Siber suç

Siber suçların tartışılmasında gerçek hukuk ile siber hukuk arasında bir ikilem vardır. Gerçek hukuk yaklaşımı, bir siber suçun çevrimdışı bir suçla aynı olduğunu ancak dijital araçlar kullanılarak yapıldığını vurgulamaktadır. Suç aynı, sadece araçlar farklıdır. Siber hukuk yaklaşımı, siber suçun benzersiz unsurlarının, özellikle uygulama ve önleme söz konusu olduğunda, özel işlem gerektirdiğini vurgulamaktadır.

CoE [Siber Suç Konvansiyonu](#) taslağı, siber suçun tek özel yönünün suç işlemek için ICT kullanımı olduğunu vurgulayarak konuyu gerçek hukuk yaklaşımına daha yakın hale getirmişti. 1 Temmuz 2004'te yürürlüğe giren konvansiyon, bu alandaki temel uluslararası araçtır.

Siber suç konusunun öne çıkması, onu bu suçların sürekli işlenmesi, elektronik ağ sistemlerini kullanarak veya onunla bağlantılı işlenmesi ve çeşitlenmesi nedeniyle, birkaç uluslararası, bölgesel ve yerel organizasyonun gündemine oturtmuştur.³⁶ Buna bir örnek, Commonwealth

İnternet Yönetişimi Forumu (CIGF) içinde doğmuş olan **Commonwealth Siber Suç İnisyatifi**'dir.³⁷ İş dünyası ayrıca siber suçlarla mücadelenin önemini kabul etmiş ve yasal hükümlerin iyileştirilmesi ve farkındalık kampanyalarını desteklemek için özel inisiyatif başlatmıştır.

Meseleler

Siber suçun tanımı

Siber suç, internet ve bilgisayar sistemleri aracılığıyla işlenen suç olarak tanımlanmaktadır. Siber suçların bir kategorisi, verilerin ve bilgisayar sistemlerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyen suçlardır. Bunlar, bilgisayar sistemlerine yetkisiz erişimi, veri iletimlerinin yasa dışı olarak durdurulması, (zarar verme, silme, bozulma, verilerin baskılanmasının değiştirilmesi gibi) veriye müdahale, (bir bilgisayarın veya başka bir cihazın işleyişini aksatmadan engelleme gibi) sisteme müdahale, sahtecilik, dolandırıcılık ve kimlik hırsızlığıdır. Diğer siber suç türleri, içerikle ilgilidir ve ulusal yasalara göre yasa dışı sayılan çevrimiçi içeriğin üretilmesini, teklif edilmesini, dağıtılmasını, satın alınmasını ve bulundurulmasını içerir. Bunlar, çevrimiçi çocuk cinsel taciz materyali, terörle ilgili bir eylemi savunan materyal, (nefreti teşvik eden materyal, şiddeti veya terör eylemlerini teşvik eden materyal gibi) aşırı uç materyal, (teknolojiyi kullanarak saldırgan, tehditkar veya taciz edici davranışlarda bulunmak gibi) siber zorbalıdır.

Siber suç ve insan haklarının korunması

Siber Suçlar Sözleşmesi, güvenlik ve insan hakları arasındaki denge hakkındaki tartışmayı gündeme getirmiştir. Sivil toplum aktörleri, Sözleşme'nin devlet yetkililerine kişisel bilgisayarları kontrol etme, iletişimin gözetim ve denetimini sağlama hakkı da dahil olmak üzere çok geniş bir güç sağladığına dair endişelerini dile getirmişlerdir. Bu geniş yetkiler bazı insan haklarını, özellikle de mahremiyeti ve ifade özgürlüğünü tehlikeye sokabilir.³⁸ Sözleşmeyi tevd eden CoE'nin insan haklarını aktif olarak teşvik etmesi, siber suçla mücadeleyle insan haklarının korunması arasında gerekli dengenin kurulmasına yardımcı olabilir. Bu bağlamda, Konsey Bakanlar Komitesinin, 2014 yılında, **üye devletlere İnternet kullanıcıları için insan hakları rehberine** ilişkin bir Tavsiye Kararı kabul ettiğini, bu rehberin diğer hükümlerin yanı sıra, "hiç kimsenin internet kullanımında insan hakları ve temel özgürlüklerinden yararlanırken yasaya aykırı, gereksiz ve orantısız müdahaleye tabi olmaması gerektiği" hükmü takdire şayandır.³⁹

Delil toplamak ve saklamak

Siber suçlarla mücadelede ana zorluklardan biri, mahkemedeki davalar için kanıt toplamaktır. Günümüz iletişiminin hızı, kolluk kuvvetlerinin hızlı yanıt vermesini gerektirmektedir. Kanıtların korunmasına yönelik bir olasılık, belirli İnternet kaynaklarına kimin eriştiği ve ne zaman yaptıkları hakkında bilgi sağlayan ağ kayıtlarıdır. Siber Suçlar Sözleşmesi, İnternet trafik verilerinin korunması yükümlülüğünü belirlemektedir.

Siber tehditlerin ve terörist saldırıların artan baskısı altında, AB bir adım daha ileri gitmiş ve 'her üye devlet tarafından kendi ulusal hukukunda tanımlandığı gibi ciddi suçların soruşturul-

ması, tespit edilmesi ve kovuşturulması amacıyla' ISS'lerin trafik ve konum verilerini tutmalarını gerektiren bir Veri Tutma Direktifi kabul etmiştir.⁴⁰ Bu hüküm gizlilik gerekçesiyle güçlü eleştirilere maruz kalmıştır ve bazı devletler direktiflere uymak için ulusal yasaları çıkarmayı başaramamış veya anayasaya aykırı olan bazı yasalar çıkarmışlardır.⁴¹ Aralık 2013'te CJEU, Temel Haklar Şartı ile uyumlu olmayan Veri Saklama Direktifini ilan etmiştir.⁴²

www.igbook.info/cybercrime

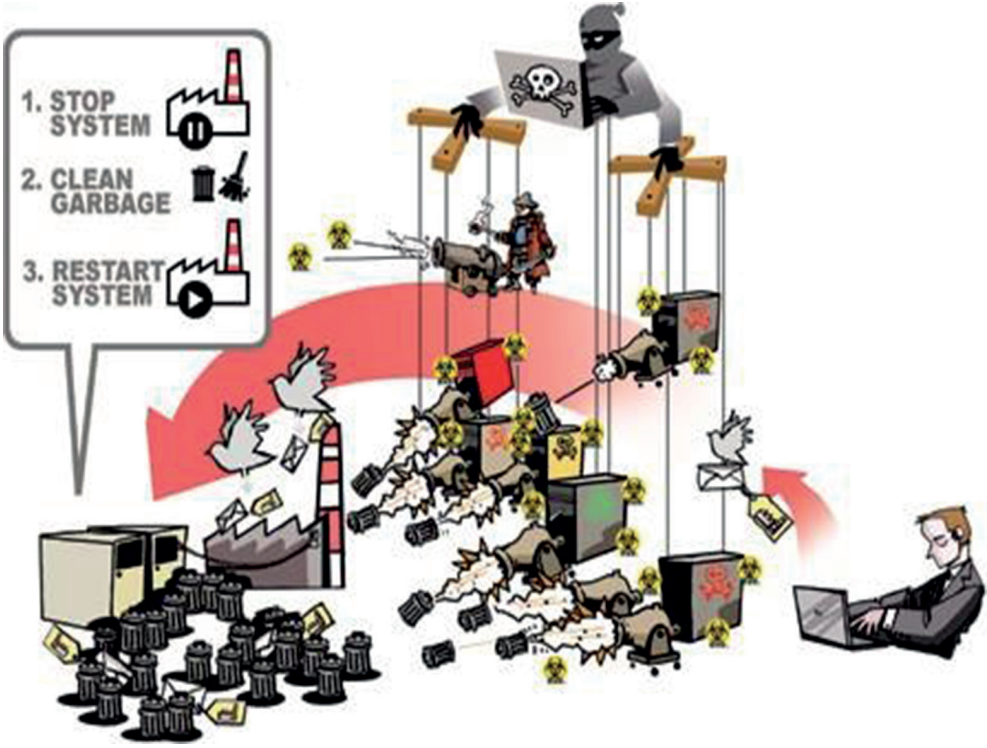
Kritik altyapı

Avrupa Komisyonuna göre, Kritik Altyapı (CI), 'halkın sağlığını, güvenliğini, emniyetini, ekonomik refahını' veya 'devletlerin etkin işleyişini' tehlikeye sokabilecek 'fiziksel teknolojik imkanlar ve bilgi teknolojisi imkanları, ağları, hizmetleri ve varlıkları' içermektedir.⁴³ Bu gibi altyapıların örnekleri arasında enerji, ulaşım ve su temini, iletişim, finans ve sağlık hizmetlerinin yürütüldüğü alt yapılar yer almaktadır. Ülkeler kendi ulusal bağlamlarına bağlı olarak kendi CI'lerini tanımlarlar. Gelişmiş ülkelerin çoğu zaten böyle bir adım atmış ve CI'larını tanımlamış olsalar da, bu henüz gelişmekte olan birçok ülke için geçerli değildir.

Giderek daha fazla, CI, (denetleyici kontrol ve veri toplama (SCADA) endüstriyel kontrol sistemleri gibi) dijital kodlara dayanan ve (Intranet veya genellikle kamusal internet yoluyla bağlanan sanal özel ağlar gibi) IP tabanlı ağlar üzerinden bağlanan kontrol sistemlerine dayanmaktadır. Bu durum, kaynak optimizasyonuna imkan sağlarken, aynı zamanda CI'yı siber saldırı riski altında bırakmaktadır. Bu tür saldırılar, DDoS saldırılarını (Şekil 14), endüstriyel sistemler üzerindeki uzaktan kontrolü, hassas bilgilerin toplanmasını veya Stuxnet virüsü ile 2014 sonunda bir Alman çelik fabrikasına yapılan siber saldırıda olduğu gibi kontrol sırasında komut parametrelerini değiştirerek tesislerin düzenli çalışmasını engellenmesini içerebilir.⁴⁴

Kritik (bilgi) altyapısının korunması

CI'nin belirli bir alt grubu CII'dir. IETF Güvenlik Sözlüğü, CII'yi "çalışmamaları veya yıkılmaları halinde, ulusal güvenlik, ekonomi veya kamu sağlığı ve güvenliği üzerinde zayıflatıcı bir etki" yaratan bir ulus için çok hayati öneme sahip sistemler olarak tanımlamaktadır.⁴⁵



Şekil 14. Kritik altyapıya DDos saldırısı

CII koruması, afet ve acil durumların önlenmesi, hazırlanması, yanıtlanması ve kurtarılmasıyla ilgili kuralları, stratejileri, planları ve prosedürleri ifade eder. Genellikle, CII'yi korumak için birkaç strateji bir araya getirilir. Bu stratejiler, kolluk kuvvetleri ve suç önleme, terörle mücadele, ulusal güvenlik ve savunma, acil durum yönetimi, iş sürekliliği planlaması, koruyucu güvenlik, e-güvenlik, doğal afet planları ve hazırlıkları, risk yönetimi, profesyonel ağ oluşturma, piyasa düzenlemesi, planlama ve altyapı geliştirme ve örgütsel esneklik gibi hususları ele almaktadır.

ABD'de, Başkanlık Politikası Direktifi (PPD21) 2013'ün Kritik Altyapı 2013'ün Güvenliği ve Esnekliği⁴⁶ hem fiziksel hem de sanal sistemleri kapsamaktadır. AB'de, Avrupa Kritik Altyapı Koruması Programı (EPCIP)⁴⁷ ve Avrupa'nın kritik altyapılarının belirlenmesi ve isimlendirilmesine ilişkin Direktif⁴⁸, kilit unsur olarak ICT sektörüne odaklanmaktadır. AB Siber Güvenlik Stratejisi ile eşleştirilmiş ağ ve bilgi güvenliği ile ilgili AB Direktifi, CERT'lerin oluşturulması da dahil olmak üzere, CIIP önlemleri konusunda üye devletlere daha spesifik bir rehber oluşturmuştur. Aynı zamanda, AB Ağ ve Bilgi Güvenliği Ajansı (ENISA), CIIP önlemlerinin uygulanmasını takip etmek ve kapasite artırıcı önlemler ve kaynaklar sağlamaktan sorumlu kılınmıştır.

OECD'nin kritik bilgi altyapılarının korunmasına ilişkin Konsey Tavsiyesi⁴⁹, üye devletlerin CII'lerini korumak için atabilecekleri birkaç adımı özetlemektedir. Ulusal düzeyde, devletler, diğerlerinin yanı sıra, ulusal stratejiler geliştirmeye, CIIP'den sorumlu devlet kurumlarını ve

organizasyonlarını tanımlama, bağımsız CERT'ler dahil olmak üzere önleme ve müdahale için organizasyon yapıları geliştirmeye, özel sektöre danışmaya ve güvenilir PPP'ler oluşturmaya davet edilmektedir. Uluslararası düzeyde, devletler bilgi paylaşımını arttırmaya ve CIIP'ten sorumlu kurumlar arasındaki işbirliğini güçlendirmeye teşvik edilmektedir.

www.igbook.info/critical

Siber terörizm

Siber terörizmin çeşitli tanımları vardır. Birçoğu basitçe bilinen terörizm tanımını kullanmış ve bunu sanal dünyaya uygulamıştır. Terörizmi tanımlayan, ancak siber terörizmin yasal bir tanımını bulunmayan İngiltere gibi ülkeler vardır.⁵⁰ Akademik çevrelerce, biraz dar da olsa 'siber terörizmin bilgi teknolojisinin ve araçlarının terörist gruplar ve taraflarca kullanılması olduğunu' belirten bir tanım yapılmaktadır.⁵¹ Daha kapsamlı ve daha geniş bir tanım, siber terörizmin, "bir hükümetin veya halkının siyasi veya sosyal hedeflere ulaşmasını engellemek için yıldırma veya zorlama maksadıyla bilgisayarlara, ağlara ve burada depolanan bilgilere karşı yapılan yasadışı saldırılar ve saldırı tehditleri" olduğunu belirtmektedir.⁵²

Uygulamada, siber terörizmin, aşağıdaki üç unsurdan birini veya daha fazlasını içerdiği anlaşılmaktadır:

- İnternetin terörist grupların saldırıları için kullanılması (DoS saldırıları, korsanlık saldırıları).
- İnternetin terörist saldırıların hazırlanması ve düzenlenmesi için kullanılması.
- Teröristlerin internetin kendilerini tanıtmak ve teröristleri işe almak için kullanması.

Terörist propaganda ve şiddet içeren aşırılık yanlısı materyallerin çevrimiçi dağıtımına karşı koyma

Terörist propaganda ve şiddet içeren aşırılık yanlısı malzemelerin çevrimiçi dağıtımı, uluslararası politikalarda ve internet şirketleri için endişe nedeni olarak tekrarlanan bir tema haline gelmiştir.

Teröristler sosyal medyayı kullanma konusunda giderek daha sofistike hale geldikçe ve bu çevrimiçi platformlar dünya çapında giderek daha fazla insana ulaşabildiğinden, çevrimiçi radikalleşme tehdidi birçok karar vericinin odağına yerleşmiştir. Nisan 2016'da Çin, Hindistan ve Rusya'nın dışişleri bakanları, çevrimiçi terörist içeriğin yükselişine karşı koyma gereğini vurgulayan ortak bir açıklama yaptılar.⁵³ Bu konu ayrıca terörizmin anlatılarına ve ideolojilerine⁵⁴ karşı koyma konusunda açık bir oturum düzenleyen BM Güvenlik Konseyi'nin gündemine gelmiş ve Mayıs 2016'da Japonya'daki G7 liderleri⁵⁵ tarafından da ele alınmıştır.

Siyasi düzeyde tartışmalara ek olarak, konu, özellikle internet endüstrisi olmak üzere özel sektör için de endişe kaynağı haline gelmiştir. Mayıs 2016'da Microsoft, çevrimiçi bir terörist içerikle ilgili politikalарını yayınlamıştır. Çünkü 'korkunç eylemlerde dolaylı olarak sorumluluk' hissetmiştir.⁵⁶ Google'ın teknoloji inkübatörü Jigsaw, arama motoru algoritmalarını değiştirerek,

terör propagandası için çevrimiçi aramalarda kullanıcıyı terör karşıtı içeriğe yönlendirebilecek şekilde YouTube videoları denemektedir.⁵⁷

Aşırı-karşıt kampanyaların uygulamadaki işleyişi, ifade özgürlüğü hakkı ile çok dikkatli bir şekilde dengelenmelidir. Güvenliği korumak ve çevrimiçi sansürü teşvik etmek arasında hassas bir çizgi vardır ve bu çizgi oldukça yoruma açıktır. Bu kaygı, “şiddet içeren aşırılıkçılık”ın hükümetler tarafından ifade özgürlüğünü sınırlamak için “mükemmel bahane” olarak kullanılabileceğini iddia eden BM İfade Özgürlüğü Özel Raportörü David Kaye tarafından vurgulanmıştır.⁵⁸ Mümkün olan en yüksek ifade özgürlüğü seviyesini sağlayan ve radikalleşmeyi en aza indirgeyen içerik politikası için doğru formül ancak güvenlik ve insan hakları toplulukları arasındaki diyalogla bulunabilir.

Siber terörizmle mücadele inisiyatifleri

Siber terörizmin tanımı konusunda anlaşmaya varılmaması yanlış yorumlamaya neden olabilir ve küresel çapta tehditleri ve olayları azaltmak için işbirliğini etkileyebilir. Ancak, buna rağmen, ülkeler siber terörizm tehdidini ciddiye almaya başlamıştır. 2012 yılında ABD Savunma Bakanlığı’nın, suç gruplarının ve bilgisayar korsanlarının İnternet üzerinde nasıl etkileşime girdiğini tespit ederek ‘siber terörizm olaylarını’ öngörecektir yazılımın geliştirilmesine yönelik teklifleri kabul ettiği bildirilmiştir.⁵⁹ Hollanda Güvenlik ve Adalet Bakanlığı’nın 2011-2013 yılları arasında yürüttüğü Temiz IT Projesi, “hükümetin, işletmelerin ve sivil toplum arasında İnternetin terörist kullanımını nasıl azaltacağını araştırmak için yapıcı bir diyalog başlatmayı” amaçlamıştır. Proje bir dizi genel ilke ve en iyi uygulamaların değerlendirilmesi ile sonuçlanmıştır.⁶⁰

Ayrıca BM siber terörizm konusuna daha fazla dikkat etmektedir. Eylül 2006’da UNGA, üye devletlerin, diğer konuların yanında, uluslararası ve bölgesel düzeylerde terörizmin İnternet üzerindeki tüm şekil ve tezahürlerine karşı koyma çabalarını koordine etmeyi taahhüt ettiği **BM Küresel Terörle Mücadele Stratejisini**⁶¹ kabul etmiştir. Sonuç olarak, stratejinin uygulanmasına ilişkin BM sisteminin faaliyetlerini koordine etmek için, Terörle Mücadele Uygulama Görev Gücü içerisinde , İnternetin Terörist Amaçlarla Kullanımına Karşı Koyma konusunda bir Çalışma Grubu oluşturulmuştur.

2012 yılında, Çalışma Grubu, UNODC ile işbirliği içinde, İnternet ile ilgili terör davalarının cezalandırılması, soruşturulması ve kovuşturulmasına ilişkin ulusal ve uluslararası düzeylerde mevcut yasal çerçeveleri ve uygulamaları araştırırken, bunun için bir dizi öneri hazırladığını bildiren bir rapor yayınlamıştır.⁶² Birleşmiş Milletler Güvenlik Konseyi Terörle Mücadele Komitesi de İnternetin terör amaçlı kullanımına ilişkin yönleri ve konuları ele almaktadır. Aralık 2015’te, BM üye devletleri, İnternet şirketleri ve sivil toplum örgütleriyle, teröristlerin terörist temin etmek için İnternet ve sosyal medyayı sömürmelerini ve terör eylemlerini teşvik etmelerini, terörist faaliyetleri kışkırtmalarını engellerken, insan haklarına ve temel özgürlüklere saygıyı esas alan bir toplantı yapmıştır. Toplantıda devletlerin ve özel sektörün, terörist amaçlı siber alan kullanımını, insan haklarının uluslararası araçlarıyla uyumlu bir şekilde nasıl önleyebileceği ve bunlarla nasıl mücadele edebileceği konusunda önerilerde bulunmuştur.⁶³

Siber çatışma ve savaş

Var olan uluslararası hukuk, geleneksel silahlı çatışma davranışını düzenlemekte ve etkilerini sınırlamayı amaçlamaktadır. Mevcut uluslararası yasal çerçevelerin çevrimiçi çatışmalar için de geçerli olduğu konusunda artan bir uzlaşma olsa da, bu çerçevelerin uygulamada nasıl işleyeceği çok açık değildir.

Ek bir zorluk, siber uzayda bir savaş eylemini neyin oluşturduğu konusunda ortak bir anlayışın bulunmamasıdır. Muhtemel bir tanım, siber savaşın “bir ulus devletin zarar verme veya bozma amacıyla başka bir ülkenin bilgisayarlarına sızma eylemlerini” içerdiğini öne sürmektedir.⁶⁴ Bununla birlikte, özellikle kilit küresel güçler arasında tanımlar konusunda bir uzlaşma yoktur.

Siber saldırıların temel bir özelliği, (botnet’ler dahil) birkaç proxy katmanı boyunca kullanılan çok karmaşık ve sofistike silahlar nedeniyle, bırakın devletlere atfetmeyi, bazı faillelere atfetmek de neredeyse imkansızdır. Dahası, geleneksel savaşların aksine, siber çatışmalar, diğer ülkeler sessizce izlerken, iki ülke arasında gerçekleşmez. İnternet küresel bir kaynaktır ve botnet’ler gibi siber silahlar, diğer ülkelerin bilgisayar kaynaklarını kendi rızası olmadan kullanır ve siber savaşları etkili bir şekilde küresel hale getirir.

Siber çatışma ve savaşla ilgili büyük siyasi tartışmalar başlatan dönüm noktası olay, Estonya’nın Nisan 2007’de yaşadığı ülke çapındaki saldırılardır. Estonya, İnternet altyapısı, dışişleri ve savunma bakanlıkları, önde gelen gazeteler ve bankalara DDoS saldırıları yaşadı.⁶⁵ Dolaylı kanıtlar, saldırılar ve Rusya’nın Tallinn’deki bir Sovyet askerleri anıtının yer değiştirmesine muhalefet edenler arasındaki bağlantılara işaret etmesine rağmen, Rus yetkililerin saldırılara katıldığı konusunda net bir kanıt bulunamamıştır. Siber savaşla daha sık ilişkilendirilen bir durum, 2008’de Rusya ve Gürcistan arasındaki ihtilaf sırasında Gürcü çevrimiçi medyasına ve hükümet sunucularına yapılan saldırıdır. Rusya tarafından devlet destekli bir saldırıya dair kanıt bulunmasa da, durum ‘siber savaş’⁶⁶ olarak anılmıştır.

ABD ve İsrail hükümetleri, siber silahların sistematik kullanımını ortaya koyan, İran’ın ana nükleer zenginleştirme tesislerini yöneten bilgisayar sistemlerine siber saldırılara dahil olduklarıyla ilgili haberler yaptılar.⁶⁷ İran, ABD’nin daha önceki eylemlerine misilleme amacıyla ABD bankalarına ve şirketlerine saldırı yapmakla suçlanmıştır.⁶⁸ ABD hükümetinin, Kuzey Kore’yi 2014 yılının sonlarında Sony’yi hacklemekle suçlaması, ABD’nin ekonomik yaptırımları ile bir adım daha ileri gitmiştir.⁶⁹

Siber savaşta daha sinsi yaklaşımlar da görülmüştür. ABD, Çin’i hükümet ve (Google ve Microsoft gibi) kurumsal bilgi altyapılarına karşı siber casusluk faaliyetlerini sistematik olarak başlatmakla suçlamıştır ki, Çin bunu reddetmiştir.⁷⁰ ABD merkezli güvenlik şirketi Mandiant’ın 2014 raporları, genişleyen Çinli siber casusluk girişimlerinin ayrıntılarını açıkladığında, Çin, kendisinin kurban olduğunu iddia ederek bunu Snowden’in ortaya çıkardığı bir PRISM gözetim programına bağlamış ve bu olayların Çin - ABD işbirliğini tehlikeye attığını belirterek uyarılmıştır.⁷¹

Hibrid savaşlarda siber saldırılar

2015 Münih Güvenlik Konferansı'nın çıktıları, siber saldırıları hibrid savaşın önemli bir parçası olarak görmektedir.⁷² Gerçek savaşı tetiklemeden barış zamanında rakibin istikrarına ve büyümesine zarar vermeyi amaçlayan siber operasyonlara atıfta bulunmaktadır.

Çatışmalar ve sınır ötesi saldırılar için botnetleri ve benzeri güçlü İnternet tabanlı silahları kullanmak, geleneksel savaşla aynı hedefe sahiptir: başka bir bölgenin ekonomik kaynaklarını kazanmak veya düşman kaynaklarını yok etmek. Siber silahlar, elektrik şebekeleri, hava trafik kontrol ağları veya nükleer santral güvenlik sistemleri gibi kritik altyapıların kontrol sistemlerini hedefleyebilir (Şekil 15).



Şekil 15. Siber silahlar

Siber saldırılarla ilgili spesifik olan, düşmanlarına saldırmanın uygun maliyetli bir yolu olmalarıdır. Örneğin, araştırmalar ülke çapında DDoS saldırısı gerçekleştirebilecek sağlam ve güçlü DDoS tesislerine yapılan yatırımın birkaç bin Euro'nun üstüne çıkmasına gerek kalmazken, böyle bir saldırının ekonomik zararının Sırbistan gibi bir geçiş ülkesi için günde 10 milyon Avrodan, İsviçre gibi gelişmiş bir ülke için günde yarım milyar Avroya değişebileceği görülmektedir.⁷³ Böylece, siber silahlar sınırlı kaynaklara sahip oyunculara ilave güç sağlayabilmektedir.

Siber silahlar, bağımsız bir savaş yöntemi olarak değil de geleneksel operasyonlara ek bir yöntem olarak kullanılabilir.

Şifreleme

Şifreleme, elektronik dokümanların şifrlenmesi ve kod çözme işleminden sonra erişilebilecek şekilde okunaksız bir biçimde iletilmesi anlamına gelir. Geleneksel olarak, sadece hükümetler, askeri ve diplomatik iletişimlerinde güçlü şifreleme geliştirmeyi ve kullanmayı bilen ve bu bilgiye sahip olan oyunculardı. Şifreleme, Pretty Good Privacy gibi uygulamalarla İnternet kullanıcıları için ekonomik hale gelmiştir. Son zamanlarda, Silent Circle, Telegraph ve Proton da dahil olmak üzere iletişimde şifrelemeli koruma sağlayan birçok platform bulunmaktadır. Ayrıca, İnternet şirketleri iç iletişimini ve kullanıcı verilerini korumak için güçlü şifreleme kullanmaya başlamışlardır.

Şifrelemenin temel olarak suçlular ve teröristler de dahil olmak üzere tüm İnternet kullanıcıları için ekonomik hale gelmesi, şifreleme araçlarının olası yanlış kullanımı dünya çapında hükümetler ve işletmeler arasındaki dijital politika tartışmalarından birini tetiklemiştir. Bu tartışmanın özü, İnternet kullanıcılarının iletişiminin gizliliğine saygı gösterme ihtiyacı ile hükümetlerin ulusal güvenlikle ilgili (potansiyel suç ve terör eylemleri bir sorun olmaya devam etmektedir) bazı iletişim türlerini izlemelerine duyulan ihtiyaç arasındaki doğru dengeyi vurgulamaktır.

Temel uygulamalar

Şifrelemeyi, çoğu zaman iletişimin gizliliğini korumak için bir araç olarak görüyoruz. Bir yandan, bilgisayarımızda veya bulutta depolanan içeriği, şifreleme araçlarını kullanarak şifrelemiz gerekmekte veya bulut servis operatörlerimizden içeriklerimizi şifrelemelerini talep etmekteyiz. Öte yandan, içeriği (bir sosyal ağ web sitesinde veya bir arkadaşınızın posta kutusu olsun) bilgisayarla hedef arasında dolaşırken de şifrelemeliyiz. Şifreleme işlemi zaman ve hesaplama kapasiteleri gerektirdiğinden, çoğu zaman gerçek zamanlı olarak şifrelemeleri gereken veri kütlesi nedeniyle şifreleme çoğu kamusal bulut veya iletişim hizmetleri sağlayıcılarının varsayılan ayarı olmayabilir. Ancak giderek daha fazla sayıda şirket şifrelemeyi, müşterilerin artan taleplerini karşılayabilecek ve böylece rekabet edebilirliklerini artırabilecek isteğe bağlı bir teklif olarak görüyor. Apple ve WhatsApp örnekleri önde gelen örneklerdir. Ayrıca, Tor ağı (trafik analizi ve gözetimini anonimleştirmek ve gizlemek suretiyle gizliliği ve temel özgürlükleri korumak için geliştirilen açık bir yazılım) gibi şifrelemeye dayalı çevrimiçi anonimlik için çeşitli ve ücretsiz kaynaklı yazılım çözümleri de bulunmaktadır.

Şifreleme, önemli İnternet protokollerinin ek güvenliği için de kritik bir bileşendir. IPSec, DNSSEC ve Sınır Ağ Geçidi Protokolü Güvenliği (BGPsec), IP numaralarının, etki alanı adlarının ve seçilen rotaların kimliğini doğrulayabilen ve makyajlı sunucular tarafından yanıltılmayı ve sahte kimliğe bürünmeyi engelleyebilecek sunucular ve yönlendiriciler için dijital sertifikaların dağıtımına dayanır. Benzer şekilde, SSL (Güvenli Yuva Katmanı), bir web sunucusu ile bir tarayıcı arasında şifrelenmiş bir bağlantı kurarak, ikisi arasındaki iletişimin gizli ve ayrılmaz kalmasını sağlar.

Şifreleme ve standartlaştırma

Bilgisayarların hesaplama gücünün gelişmesi, daha hızlı şifrelemeye olanak sağlar, ancak aynı

zamanda daha hızlı kriptanaliz ve standartların daha sık değişmesini de sağlamaktadır. Ticari ürünlerde uygulanmasının fiili standart haline getirilmesi gereken en karmaşık algoritmaların hangisi olduğu kararı, IETF, Amerikan Ulusal Standartlar Enstitüsü ve (kriptografiye yatırım yapabilen) ekonomik olarak en güçlü ulusların ABD Ulusal Standartlar ve Teknoloji Enstitüsü gibi standartlarla ilgilenen kar amacı gütmeyen ulusal standardizasyon kuruluşlarındaki mühendisler ve bilim adamları tarafından verilmektedir. İnternet sürveyansına yönelik artan jeopolitik ilgiyle birlikte, kitlesel şifreleme kullanımına yönelik çeşitli eğilimlerle karşı karşıya kalan ulusal güvenlik hizmetleri, bilim insanının yönlendirdiği standardizasyon süreçlerine daha fazla ilgi göstermeye başlamıştır: Snowden'in açıklamalarından sonra, Der Spiegel, 'NSA'nın bu tür standartları geliştiren bir kuruluş olan İnternet Mühendisliği Görev Gücü'nün (IETF) toplantılarına bilgi toplamak ve muhtemelen tartışmaları da etkilemek için için seyahat ettiklerini rapor etmiştir.⁷⁴

Şifreleme araçları araçları için uluslararası usuller

Şifreleme politikasının uluslararası yönleri, güvenlik ve işletme seviyelerinde koordinasyonu içermektedir.

Örneğin, ABD şifreleme yazılımının ihracat kontrolü politikası çok başarılı değildi çünkü uluslararası dağıtımını kontrol edemedi. ABD yazılım şirketleri, ihracat denetimlerinin ulusal güvenliği artırmadığını, aksine ABD'nin ticari çıkarlarına zarar verdiğini savunarak güçlü bir lobi kampanyası başlatmıştır.

Şifreleme iki bağlamda ele alınmıştır: Wassenaar Düzenlemesi ve OECD. [Wassenaar Düzenlemesi](#), 41 ülke tarafından konvansiyonel silahların ve "ikili kullanımlı" teknolojilerin savaş halindeki veya "parya devletleri" olarak düşünülen ülkelere ihracatını sınırlamak için kabul edilen uluslararası bir rejimdir.⁷⁵ Anlaşmayla Viyana'da bir sekreteryaya kurulmuştur. Wassenaar Grubu ile birlikte ABD lobisi, [Kısıtlama Yaklaşımını](#)⁷⁶ şifreleme yazılımını kilit bir emanet üzerinden kontrol ederek uluslararası alana genişletmeyi amaçlamıştır. Buna, başta Japonya ve İskandinav ülkeleri olmak üzere birçok ülke tarafından direnilmiştir.

1998 yılında, 56 bitin üzerinde donanım ve yazılım kriptografi ürünlerinin çift kullanımlı kontrol listesini içeren kriptografi kılavuzlarının tanıtılması yoluyla bir uzlaşmaya varıldı. Bu uzantı, web tarayıcıları ve e - posta gibi İnternet araçlarını içeriyordu. Bu düzenlemenin, indirme gibi 'maddi olmayan' transferleri kapsamadığını not etmek ilginçtir. Clipper'in uluslararası bir versiyonunun tanıtılmaması, bu teklifin ABD'de kendi içinde geri çekilmesine katkıda bulunmuştur. Ulusal ve uluslararası arenalar arasındaki bağlantının bu örneğinde, uluslararası gelişmeler ulusal olanlar üzerinde belirleyici bir etkiye sahip olmuştur.

OECD, şifreleme alanında uluslararası işbirliği için bir diğer forumdur. OECD yasal olarak bağlayıcı belgeler üretmemesine rağmen, çeşitli konularda onun rehberlerine büyük saygı duyulmaktadır. Bunlar uzman yaklaşımının ve fikir birliğine dayalı karar alma sürecinin bir sonucudur. Kurallarının çoğu nihayetinde ulusal yasalara dahil edilmiştir. Şifreleme sorunu OECD faaliyetlerinde oldukça tartışmalı bir konu olmuştur. 1996 yılında ABD'de, uluslararası bir standart olarak (belirli yükümlülükler yerine getirilene kadar bir şeyin üçüncü kişiye emanet

edilmesi anlamına gelen) temel bir emanet önerisini ortaya koymuştur. Wassenaar'a benzer şekilde, ABD'nin uluslararası standartlarla temel emanet önerisine ilişkin müzakerelere Japonya ve İskandinav ülkeleri tarafından şiddetle karşı çıkmıştır. Sonuç, ana şifreleme politikası öğelerinin uzlaşma şartnamesi olarak ortaya çıkmıştır.

Özellikle Wassenaar Düzenlemesi bağlamında şifreleme için uluslararası bir rejim geliştirme girişimleri, etkili bir uluslararası rejimin gelişmesine yol açmamıştır. İnternette güçlü şifreleme yazılımı elde etmek hala mümkündür.

Güvenlik ve insan hakları meseleleri

Şifreleme vatandaşların gizliliklerini korumalarını sağlar. Şifreleme, suçlular ve teröristler tarafından iletişimlerini korumak için de kullanılır. Bu kişiler 2015'te Paris'teki terörist saldırılarda⁷⁷ olduğu gibi, İnternet üzerinden silah satın alma gibi lojistiği desteklemek için İnternet'i kullanma konusunda giderek daha yetenekli hale gelmektedir. Bitcoin gibi kripto para birimleri aracılığıyla para transferi ile anılan karanlık ağa (dark web) erişmek için halka açık anonim proxy sunucularının ve Tor gibi adsızlaştırma hizmetlerinin kullanılması çok az iz bırakmakta ve çevrimiçi gözetim ve dijital takibi oldukça karmaşık hale getirmektedir. Ayrıca, dünyanın dört bir yanındaki ifşacı ve muhalif aktivistlerin hayatlarını koruyan iPhone veya Sessiz Çember (Silent Circle) gibi son teknoloji şifreleme araçları ve Telgraf veya Sinyal gibi şifreli sohbet için geliştirilen çeşitli mobil uygulamalar mobil cihazları giderek daha güvenli hale getirmekte, ancak aynı zamanda iletişimlerinin açığa çıkmasından çekinen teröristler tarafından kendi içlerindeki koordinasyonun sağlanmasında güvenli bir zemin oluşturmaktadır.

Buna karşılık, İngiltere, Fransa ve ABD de dahil olmak üzere pek çok ülkedeki hükümetler ve güvenlik hizmetleri, ana ürün ve hizmetlerdeki şifreleme algoritmalarının gücüne sınır koymaya ve devlet kurumlarının eğer gerekliyse şifreli verilere erişmesine izin verecek mekanizmalar oluşturmaya çalışmaktadır. Ayrıca, ABD, İngiltere ve Rusya gibi bazı ülkeler de, teknoloji şirketlerinin kolluk kuvvetlerinin (az veya çok tanımlanmış koşullarda) şifreli veri ve/veya cihazlara erişmesine izin verecek veya bu tür verilere erişmelerinde onlara yardımcı olunması için özel yasalar çıkarmaya çalışmaktadır. Hükümetler, şifreli verilere erişimin, ciddi suçları önleme ve kovuşturma, kamu güvenliğini sağlama amaçları bakımından giderek daha önemli hale geldiğini savunmaktadır.

Sivil toplum ve insan hakları toplulukları, bu tür önlemlerin siyasi dsndür ve orantısız gözetim için kullanılabileceğini ve ayrıca otoriter devletlerdeki gazetecilerin, blog yazarlarının ve siyasi aktivistlerin bireysel güvenliklerini tehlikeye atacağını ileri sürerek Snowden'in ifşalarıyla da beslenen bu endişelerden de rahatsız olduklarını belirtmektedirler. Ayrıca, yasa koyucu kurumların iddia ettiği gibi şifrelemenin suçluları koruyamayacağı⁷⁸ ve zorunlu arka kapıların şifreli ürünlere sokulmasının etkisiz olacağı ileri süren çalışmalar da bulunmaktadır.⁷⁹

İnsan hakları bakış açısından, gizlilik ve diğer insan hakları hakları korunmalı ve yaygın şifreleme dahil olmak üzere şifreleme araçları gizliliği korumak için esas alınmalıdır. Şifreleme ve anonimlik için daha fazla koruma ihtiyacı, örneğin dijital çağda düşünce ve ifade özgürlüğü haklarını kullanmak için şifreleme ve anonimlik kullanımına ilişkin BM İnsan Hakları Komisyon (UNHRC) Özel Raportörünün Raporu'nda vurgulanmıştır.⁸⁰

Şifrelemenin güvenlik ve insan hakları yönleri, özellikle 2016'nın ilk yarısında çok fazla dikkat çeken, son derece kamuya açık hale gelen Apple - FBI davası sonrasında uluslararası düzeyde tartışılmaya başlanmıştır. Apple'ın FBI'nın bir iPhone'un kilidini açmasına yardım etmesini emreden bir mahkeme kararının ardından iki karşıt görüş tetiklenmiştir. Bir tarafta, diğer İnternet şirketleri ve insan hakları aktivistleri tarafından desteklenen Apple, talebe uymanın tehlikeli bir emsal teşkil edeceğini ve kullanıcılarının gizliliğini ve güvenliğini ciddi şekilde azaltacağını savunmuştur. Öte yandan yetkililer, davanın arka kapı veya cihazların şifresini çözme içermediğini, daha ziyade davada gerekli olan 'bir' kez 'çözümünü içerdiğini savunmuştur. Ayrıca Apple'ı terörle ilgili soruşturmadan ziyade ticari çıkarlarına değer vermekle suçlamışlardır. Sonunda dava düşmüş (ABD Adalet Bakanlığı, bir üçüncü tarafın yardımı ile iPhone'un kilidini açabildiğini açıkladığından), açık kalan birçok soru gündeme gelmiştir. Bir yandan, yetkililer hangi koşullar altında teknoloji şirketlerinden cihazları için oluşturdukları güvenlik sistemlerini kırmalarını isteme hakkına sahiptir? Hangi güvenceler vardır veya olmalıdır? Yetkililerin, şirketlerin ürünlerini tasarlama şeklini etkilemelerine izin verilmeli midir? Öte yandan, şirketler kullanıcılarının gizliliğini ne ölçüde korumalıdır? Neye mal olursa olsun mahremiyet korunmalı mıdır?⁸¹

Snowden'in ifşalarından sonra kaybedilen güveni güçlü şifrelemeyi varsayılan olarak kabul ederek sağlamaya çalışan İnternet endüstrisi ve dijital iletişimi çözmenin yollarını arayan ve nihayetinde şifreleme araçlarının geliştirilmesi ve uygulanmasına bir son vermek isteyen güvenlik ve istihbarat servisleri arasındaki gerilim artmaktadır. Yetkili makamların ticari sistemlerdeki mevcut güvenlik açıklarını keşfetme hakkı olmalı mıdır? Hangi koşullar altında olmalıdır? Yetkililer bir hizmetin eklenmesi için belirlenen güvenlik açıklarını kamuya veya sağlayıcıya ifşa etmek zorunda mı olmalıdır?

Bu ve benzeri diğer sorular cevapsız kalsa da, pek çok İnternet ve teknoloji şirketi ürün ve hizmetlerinde şifreleme uygulamaya ve bu şifreli ürün ve hizmetleri üreticiler için bile kırılmaz hale getirecek çözümler aramaya (bu böylece, hükümetlerden gelen şifreleme mekanizmalarını kırma veya şifreli verilere erişme taleplerini hükümsüz kılmaya) devam etmektedir.

www.igbook.info/encryption

Spam

Mevcut durum

Spam, genellikle çok sayıda İnternet kullanıcıasına gönderilen istenmeyen e-posta olarak tanımlanmaktadır. Spam, esas olarak ticari tanıtım için kullanılır. Diğer kullanım alanları arasında sosyal aktivizm, politik kampanya ve pornografik materyallerin dağıtımı ve gittikçe artan şekilde kötü amaçlı yazılımda yer almaktadır. İstenmeyen bir durumun yanı sıra, spam, hem kullanılan bant genişliği hem de kontrol etmek/silmek için harcanan zaman kaybı, aynı zamanda spam yoluyla daha sık ve daha sık gönderilen (banka hesap bilgilerinin ve diğer ekonomik olarak hassas bilgilerin çalınmasına neden olan kötü amaçlı yazılım içeriği nedeniyle de önemli ekonomik kayıplara neden olmaktadır.⁸²



Şekil 16. Spam

10 yıl önce spam, kilit yönetim sorunlarından biriydi, bugün oldukça gelişmiş teknolojik filtreler sayesinde daha az öne çıkmaktadır. 2015 istatistiklerine göre, spam 2010 yılında% 84,9'a kıyasla toplam gelen e-postanın% 54'ünü temsil ediyordu.⁸³ Ancak araştırmacılar, e-posta trafiğindeki spam düzeyinin son yıllarda sürekli azalmasına karşın kötü amaçlı içeriğe sahip e-postaların önemli ölçüde arttığı (Şekil 16) konusunda uyarılmaktadırlar. Örneğin, Kaspersky Lab, 2016 yılının ilk çeyreğinde gönderilen kötü amaçlı spam e-posta sayısının, 2015 yılının aynı dönemine göre 3,3 kat daha yüksek olduğunu fark etmiştir.⁸⁴ Örnek olarak, ilk olarak Şubat 2016'da tanımlanan 'ünlü' fidye yazılımı Trojan Locky spam e-posta mesajları ile dünyaya yayılmıştır. Nisan 2016'da gelen raporlar, 110'dan fazla ülkede kullanıcılarına Trojan'a bulaştırmak için girişimlere işaret etmektedir.⁸⁵

Spam ile, hem teknik hem de yasal yollarla mücadele edilebilir. Teknik tarafta, mesajları filtrelemek ve spam tespit etmek için birçok uygulama mevcuttur. Mesajlaşma, Kötü Amaçlı Yazılım ve Mobil Kötüye Kullanımı Önleme Çalışma Grubu (M3AAWG), Spamhaus Projesi, GSMA ve İnternet Topluluğunu kapsayan teknik bir topluluk tarafından geliştirilen birkaç en iyi uygulama bulunmaktadır.

Yasal karşılık

İstenmeyen postayla mücadele için teknik yöntemlerin yalnızca sınırlı bir etkisi vardır ve tamamlayıcı yasal önlemler gerektirir. Hukuk tarafında, birçok ülke yeni spam karşıtı yasalar getirerek tepki göstermektedir. ABD’de, **Çöp-Spam Yasası**, e-posta tabanlı tanıtım yapılmasına izin verilmesi ve spam’in önlenmesi arasında hassas bir denge kurmaktadır.⁸⁶ Yasalar, beş yıla kadar hapis cezası⁸⁷ da dahil olmak üzere spam dağıtımı için ağır cezalar öngörmesine rağmen, eleştirilenlere göre bazı hükümler, spam etkinliğini hoşgörebilmekte veya hatta teşvik edebilmektedir. Yasada belirtilen başlangıç, varsayılan konum, spam iletilerinin alıcısına (devre dışı bırakma yan tümcesi kullanarak) “dur” diyene kadar istenmeyen postanın girilmesine izin verilmesidir.

Temmuz 2003’te, AB **gizlilik ve elektronik iletişim konusundaki Direktifinin**⁸⁸ bir parçası olarak kendi spam karşıtı yasasını yürürlüğe koymuştur. AB kanunları, genel bir kural olarak, doğrudan pazarlama için e-posta gönderilmesine kullanıcıların önceden onayları varsa (tercih yaklaşımı) izin verilebileceğini öngörmektedir. Bununla birlikte, önceden var olan ticari veya ticari ilişkilerde istisnalar vardır: Kullanıcılara veri toplama sırasında veya daha sonraki aşamalarda buna itiraz etme fırsatı verilirse (vazgeçme yaklaşımı) doğrudan pazarlama için elektronik iletişim bilgilerinin kullanımına izin verilir. Yönerge ayrıca, spam’in azalmasına neden olacak öz düzenleme ve özel sektör girişimlerini de teşvik etmektedir.

Hem ABD’de hem de AB’de kabul edilen spam karşıtı yasaların her birinin bir zayıflığı vardır: Sınır ötesi spam’lerin önlenmesi için hüküm eksikliği bulunmaktadır. Benzer bir sonuca, Amsterdam Üniversitesi Enformasyon Yasası Enstitüsü’nün yürüttüğü AB’nin spam karşıtı yasası ile ilgili bir araştırmada ulaşılmıştır: “İstenmeyen postaların çoğunun AB dışından kaynaklandığı basit gerçeği, Avrupa Birliği’nin Direktifinin etkinliğini önemli ölçüde kısıtlamaktadır.”⁸⁹ Uluslararası bir antlaşma ya da benzeri bir mekanizma aracılığıyla uygulanan küresel bir çözüm gerekmektedir.

2013 yılında Avustralya, Kore ve İngiltere tarafından imzalanan bir MoU, spam karşıtı kampanyada uluslararası işbirliğinin ilk örneklerinden birisidir. Mutabakat, her ülkeden gelen spam’ı en aza indirmek ve her ülkedeki son kullanıcılara gönderilmek üzere işbirliğini teşvik etmektedir. Daha yakın bir zamanda, Haziran 2016’da, Kanada, ABD, Avustralya, Hollanda, Kore, Yeni Zelanda ve Güney Afrika’daki yetkililer arasında spam ile mücadele konusunda bir MoU daha imzalanmıştır.⁹⁰

OECD, spam konusunda bir görev gücü oluşturmuş ve bir anti-spam araç seti hazırlamıştır. Ayrıca ITU de spam’le mücadeleye yönelik bir dizi faaliyet yürütmektedir. ITR’ler, bazıları tarafından e-posta spam’i olarak yorumlanan ‘istenmeyen toplu elektronik iletişimlerin’ önlenmesine ilişkin hükümler içermektedir. Ancak, bu hükümler bağlayıcı dil içermez; bunun yerine, sadece ülkelerin “gerekli önlemleri almaya çaba göstermeleri” gerektiğini ve onları işbirliği yapmaya teşvik ettiklerini belirtirler.

ITR’ler konusunda daha fazla tartışma için 4. Bölüme bakınız.

Benzer şekilde, ITU Dünya Telekomünikasyon Standardizasyon Meclisi'nin (WTSA) 2012 kararı, devletleri spam ile mücadele için uygun adımlar atmaya davet etmekte ve sadece ulusal çerçevelere atıfta bulunmaktadır.⁹¹ Pratik tarafta, ITU, Telekomünikasyon Standardizasyon Sektörü (ITU - T) yoluyla, spam ile mücadele için uygun yöntemleri belirlemeye çalışmaktadır; örneğin, ITU T Güvenlik Çalışma Grubu 17 spam ile mücadele için potansiyel önlemler konusunda çalışmalar ve yeni spam biçimlerini kapsayan teknik öneriler geliştirmeye yönelik çalışmalar yürütmektedir. Grup tarafından ele alınan hususlar, mevcut ve gelecekteki ağlarda spam üzerine formlar, spam'in etkileri, spam oluşumunu ve yayılmasını güçlendiren teknolojiler ve spam ile mücadele için çözümler içermektedir. Bölgesel düzeyde, APEC [Spama Karşı Eylem için bir İlkeler seti](#)⁹² hazırlamıştır ve AU, [Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesine](#)⁹³ (e-posta dahil) "elektronik yollarla reklam" ile ilgili hükümler eklemiştir.

Spam ile mücadeleye adanmış bir diğer girişim, spam ile ilgili mevzuatın uygulanmasında ve çevrimiçi sahtekarlık, kötü amaçlı yazılım, phishing ve virüslerin yayılması gibi benzer zorlukların ele alınmasında uluslararası işbirliğinin çerçevesini oluşturan Londra Eylem Planıdır. 2004 yılında kurulan ağ, 25'ten fazla ülkedeki düzenleyici otoritelerin yanı sıra teknik topluluk ve iş sektörünün temsilcilerini bir araya getirmektedir.

Meseleler

Filtreleme sistemleri

Spam ile ilgili çeşitli sorunlar var. Teknik açıdan bakıldığında, filtreleme sistemleriyle ilgili ana sorunlardan biri spam olmayan mesajları da sildikleri bilinmektedir. Örneğin, Verizon'un spam karşıtı filtrelemesi, e-postalarını engellediği için meşru mesajlarını almayan kullanıcılar için rahatsızlık yarattığı için için bir davaya yol açmıştır. Bununla birlikte, spam karşıtı endüstri, spam'i düzenli iletilerden ayırabilen giderek daha karmaşık uygulamalar geliştiren, büyüyen bir sektördür.

Spamın farklı tanımları

Spam'in farklı anlaşılması, spam karşıtı kampanyayı etkilemektedir. ABD'de, konuşma özgürlüğünün korunmasına ilişkin genel endişeler ve İlk Değişiklik spam karşıtı kampanyayı da etkilemektedir. ABD yasa koyucuları spamı yalnızca "istenmeyen ticari e-posta" olarak görmek; siyasi aktivizm ve pornografi dahil olmak üzere diğer spam türlerini dışarıda bırakmaktadırlar. Diğer birçok ülkede, spam, içeriğinden bağımsız olarak "istenmeyen toplu e-posta" olarak kabul edilir. İstenmeyen postaların çoğunun ABD'den kaynaklanması⁹⁴ nedeniyle, tanımlardaki bu fark, etkili bir uluslararası spam karşıtı mekanizma geliştirme olasılığını ciddi şekilde sınırlandırmaktadır.

Spam ve e-posta doğrulama

Spam'in yapısal sağlayıcılarından biri, sahte gönderi adresiyle birlikte o adresten normal posta iletileri gönderme olasılığıdır. Mevcut İnternet e-posta standartlarında değişiklik yapılmasını

gerektiren bu sorunun olası bir teknik çözümü vardır. IETF, e-postanın onaylanmasını sağlayacak e-posta protokolündeki değişiklikleri düşünmektedir. Bu, teknik sorunların (standartların) politikayı nasıl etkileyebileceğine bir örnektir. E-posta kimlik doğrulamasının getirilmesinin getireceği bir ihtimal, İnternet üzerindeki anonimlik sınırlamasıdır.

Küresel eylem ihtiyacı

Çoğu spam, belirli bir ülkenin dışından kaynaklanır. Küresel bir çözüm gerektiren küresel bir sorundur. Gelişmiş küresel işbirliğine yol açabilecek çeşitli girişimler vardır. İki taraflı ve çok taraflı MoU'lar gibi bazılarında daha önce bahsedilmiştir. Diğer önlemler arasında kapasite geliştirme ve bilgi alışverişi yer almaktadır. Daha kapsamlı bir çözüm, bir tür küresel anti-spam aracını içerecektir. Şimdiye kadar, gelişmiş ülkeler ikili veya bölgesel spam karşıtı kampanyalarla birlikte ulusal önlemlerin güçlendirilmesini tercih etmişlerdir. Temelde gelişmiş ülkelerden kaynaklanan kamusal anlamda “küresel kötüyü” transfer eden çoğu gelişmekte olan ülke spam sorununa küresel bir yanıt aramakla ilgilenmektedir.

www.igbook.info/spam

Dijital imzalar

Genel olarak konuşursak, dijital imzalar⁹⁵ İnternet'teki kişilerin doğrulanması ile bağlantılıdır ve yargı, siber suç ve e-ticaret alanlarında önemlidir. Dijital imzaların kullanılması, İnternette güven oluşturmaya katkıda bulunmalıdır. Dijital kimlik doğrulama, genel olarak, e-ticaret sözleşmelerin kolaylaştırılmasını amaçladığı için e-ticaret çerçevesinin bir parçası olarak düşünülmektedir. Örneğin, bir e-posta yoluyla veya bir web sitesi aracılığıyla tamamlanırsa bir sözleşme geçerli ve bağlayıcı mıdır? Birçok ülkede, yasa sözleşmelerin “yazılı olarak” veya “imzalanmış” olmasını gerektirir. İnternet açısından bunun anlamı nedir? Elektronik imzalı bir belgenin bütünlüğü nasıl doğrulanabilir? Bu ikilemlerle karşı karşıya kalan ve bir e-ticareti kolaylaştıran ortam oluşturmak için baskı yapan birçok hükümet, dijital imzalarla ilgili mevzuat kabul etmeye başlamıştır.

Dijital imzalar söz konusu olduğunda asıl zorluk, hükümetlerin siber suç veya telif hakkı ihlali gibi mevcut bir sorunu düzenlememesi değil, nispeten yeni bir gelişme için yeni bir düzenleyici ortam yaratmasıdır. Bu durum, dijital imzalarla ilgili hükümlerde çeşitli çözümler ile sonuçlanmıştır. Dijital imzaların düzenlenmesinde üç ana yaklaşım ortaya çıkmıştır.⁹⁶

Birincisi, elektronik imzaların elektronik formda oldukları için reddedilemeyeceğini belirten minimalist bir yaklaşımdır. Bu yaklaşım, dijital imzaların çok geniş bir kullanımına vurgu yapar ve anglo sakson hukuk sistemini kullanan ülkelerde kabul edilmiştir: ABD, Kanada, Yeni Zelanda ve Avustralya.

İkinci yaklaşım, kriptografi ve genel anahtar tanımlayıcıların kullanımı da dahil olmak üzere dijital imzalar için bir çerçeve ve prosedürler belirten maksimalist yaklaşımdır. Bu yaklaşım genellikle gelecekteki dijital imza kullanıcılarını sertifikalandırabilen özel sertifika yetkililerinin kurulmasını vurgular. Bu yaklaşım, Almanya ve İtalya gibi Avrupa ülkelerinin kanunlarında

hakim olmuştur.

Üçüncü yaklaşım, ilk iki yaklaşımı birleştirir. Elektronik ortamda sağlanan imzaların tanınması için minimalist bir hüküm vardır. Maksimalist yaklaşım, “gelişmiş elektronik imzaların” yasal sistemde (örneğin, bu imzaların mahkeme davalarında kanıtlanması daha kolay olması gibi) daha güçlü bir yasal etkiye sahip olacağı düşünülerek kabul edilmektedir. Bu yaklaşım, AB tarafından 1999 Elektronik İmzalar Direktifi ve replasmanı, [iç pazardaki elektronik işlemler için elektronik tanımlama ve güven hizmetleri ile ilgili Yönetmelik](#) (eIDAS Tüzüğü)⁹⁷ ile kabul edilmiştir. AB yönetmeliği, gelişmiş elektronik imza kavramını yeniden tanımlamakta, elektronik güven hizmetlerini tanıtmakta ve AB genelinde birleşik bir yasal çerçeve sağlamaktadır.

Küresel düzeyde, 2001 yılında Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu (UN- CITRAL), bazı teknik gerekliliklerin yerine getirilmesi koşuluyla, el yazısı ile aynı statüde olan [Dijital İmzalar Model Kanununu](#)⁹⁸ kabul etmiştir.

Açık anahtar altyapısı (PKI) girişimleri doğrudan dijital imzalarla ilgilidir. İki kuruluş, ITU ve IETF, PKI standardizasyonu ile ilgilenmektedir.

Meseleler

Kullanıcıların tanımlanması

Dijital imzalar, İnternet’teki gizlilik ve kimlik doğrulama arasındaki ilişkinin daha geniş bir değerlendirmesinin bir parçasıdır. İnternetteki bireyleri tanımlamak için kullanılan önemli tekniklerden sadece bir tanesidir.⁹⁹ Örneğin, dijital imza mevzuatının veya standartlarının ve prosedürlerinin henüz kurulmadığı bazı ülkelerde, cep telefonları üzerinden SMS kimlik doğrulaması bankalar tarafından müşterilerin çevrimiçi işlemlerini onaylamak için kullanılmaktadır.

Detaylı uygulama standartları ihtiyacı

Pek çok gelişmiş ülke geniş dijital imza mevzuatını benimsemiş olsa da, çoğu zaman ayrıntılı uygulama standartları ve prosedürlerinden yoksundur. İlgili konuların yenilikçiliği göz önüne alındığında, birçok ülke somut standartların hangi yönde geliştiğini görmeyi beklemektedir. Standardizasyon girişimleri, uluslararası kuruluşlar (ITU ve ISO), bölgesel organlar (Avrupa Standardizasyon Komitesi - CEN, ETSI, vb.), Yerel organlar (ABD Ulusal Standartlar ve Teknoloji Enstitüsü gibi) ve profesyonel dernekler (IETF) de dahil olmak üzere çeşitli düzeylerde gerçekleşmektedir.

Teknolojik tarafsızlık

Biyometri gibi yeni elektronik imza türleri birçok ülkede giderek daha fazla kabul görmektedir. Diğer birçok alanda olduğu gibi, özellikle teknolojinin ve inovasyonun hızlı bir şekilde geliştiği alanlarda olduğu gibi, yasa koyucuların bu tür mekanizmaları kodlamak arasında bir denge kurması gerekir ve aynı zamanda teknolojinin yasalara aykırı riskten kaçınmasını önlemek için tarafsız yollarla yasalaştırılması gerekir.

Uyuşmazlık riski

Dijital imzalar alanındaki yaklaşım ve standartların çeşitliliği, farklı ulusal sistemler arasında uyumsuzluğa neden olabilir. Patchwork çözümleri, e-ticaretin gelişimini küresel düzeyde kısıtlayabilir. Gerekli uyum bölgesel ve küresel organlar tarafından sağlanmalıdır.

www.igbook.info/esignature

Çevrimiçi çocuk güvenliği

Çocukların interneti kullanımı artmaktadır. İnternet, çocuklar ve gençler¹⁰⁰ için, eğitim fırsatları, kişisel gelişim, kendini ifade etme ve başkalarıyla etkileşim kurma gibi birçok avantaj sunar. Aynı zamanda, çocukların ve gençlerin özellikle savunmasız olma riskleri de söz konusudur.

Çocuklar açısından teknolojinin yararlarının yanında, aynı zamanda emin ve güvenli bir çevrimiçi ortam sağlama konusunda paydaşların dikkatli bir denge kurmaları gerekir: bir yandan çocukların uygunsuz içeriğe ve riskli davranışlara karşı korunmaları gerekir; öte yandan, diğer hakların yanında bilgiye erişme ve konuşma özgürlüğü haklarına saygı duyulması gerekir.

Zorluklar

Çocukların teknolojiyi ve interneti nasıl kullandıklarını anlamak, çocukların çevrimiçi güvenliğine ilişkin politikaları ve girişimleri bilgilendirmek için çok önemlidir. Çevre hızla gelişmekte ve sürekli olarak çocukların yaşamları ve güvenlikleri üzerinde önemli etkiye sahip yeni teknolojiler üretmektedir. Çocukları çevrimiçi ortamda korumak için evrensel olarak uygulanabilecek tek bir plan olmamasına rağmen, davranışları ve teknoloji kullanımı politika oluşturma süreçlerine yön verir ve paydaşları harekete geçirir.

Çocuklar için çevrimiçi riskler

İnternet'in sayısız yararına rağmen, çocuklar ve gençler İnternet ve teknolojiyi kullanırken belirli çevrimiçi risklerle karşı karşıya kalmaktadır. Her yaştaki kullanıcılar risklerle karşı karşıya kalsa da, çocuklar hala gelişme sürecinde oldukları için özellikle savunmasızdır. Çeşitli tipolojilere¹⁰¹ dayanarak, aşağıdakileri riskleri özetleyebiliriz:

Uygunsuz içerik. Çocuklar, yetişkinlere yönelik içerik ve şiddet içeren içerikler dahil olmak üzere, yaşları için uygun olmayan içeriğe maruz kalabilirler. Örneğin, şiddet içeren oyunlar 'pasif' şiddet içeren filmlerde hızla baskın hale gelmekte ve gerçek silahların özelliklerini gösteren sofistike silahlar ve kan dökülmesi gibi içerikler barındırmaktadırlar.

Uygunsuz temas. Çocuklar, zorbalık ve taciz gibi zararlı temaslara maruz kalabilir ve sosyal ağlar gibi çevrimiçi iletişim araçlarını kullanırken bu tür temaslara karşı özellikle savunmasızdırlar. Çocuklar genellikle kendi yaşlıtlarının mağdurları durumuna düşmekle birlikte, uygun olmayan temas, çok daha tehlikeli biçimde potansiyel cinsel istismar faillerinin tuzağına da düşebilirler.

Uygunsuz davranış. Çocuklar ve gençler uzun vadeli 'dijital ayak izleri'nin kendileri ve başkaları için etkilerini tam olarak anlamayı başaramazlar. Uygunsuz davranış, uygunsuz yorumların

yayınlanmasını veya olumsuz sonuçlara yol açabilecek hassas kişisel bilgilerin veya görüntülerin ifşa edilmesini içerir. mobil teknoloji aracılığıyla sanal seks yapmak ya da cinsel içeriğin ağırlıklı olarak paylaşmak, giderek yaygınlaşan bir uygulamadır ve araştırmalar, gençlerin bu uygulamaya katılımları için gittikçe daha fazla baskı olduğunu göstermiştir.

Tüketici ile ilgili konular. Ticari riskler olarak da adlandırılır, tüketiciyle ilgili konular arasında uygunsuz reklamların hedef veya alıcı olması, (kullanıcıları bir hizmet almaya davet eden uygulamalar gibi) gizli maliyetlere maruz kalmak ve spam almak sayılabilir. Çocuklar ayrıca çevrimiçi konum ve coğrafi konum verileri dahil olmak üzere veri toplanmasıyla ilgili risklerle karşı karşıyadır.

Geniş kapsamlı risklere rağmen, Avrupa’da yapılan araştırmalar¹⁰², çocuklar ve gençlerin risklere daha fazla maruz kalmasına rağmen, her riskin gerçek zararlara yol açmayacağını göstermektedir. Bunların çoğu çocuğun yaşına, cinsiyetine ve risklerle başa çıkabilme esnekliğine ve kaynaklarına bağlıdır. Ebeveynler, veliler, eğitimciler, hükümet, ticaret sektörü ve diğer paydaşlar çocukları çevrimiçi ortamda korumada ve risklerle uygun şekilde başa çıkmalarına yardımcı olmada önemli bir rol oynamaktadır.

Çevrimiçi cinsel taciz ve istismar

Çocuk cinsel istismarı konusu yeni olmasa da, İnternet sorunu daha da kötüleştirmiştir. Avcılar genellikle eğilimlerini anonim olarak keşfedebilir ve yasal yaptırımlardan kaçma yollarını bulabilirler. Burada açıklanan çevrimiçi risklerin bazıları, bir tür cinsel şiddete neden olabilir: avcılara yakalanan çocuklar hazırlanmaya ve cinsel istismara konu olabilir; bu çocuklar kimliği belirsiz kişilerce kendilerinin cinsel imajlarını yaratmaya ve paylaşmaya ikna edilme gibi saldırılara maruz kalabilirler ve bu daha sonra onları taciz etmek veya tehdit etmek için kullanılabilir.

Çocuklar ve gençler sıklıkla istismarcılar tarafından da kullanılan sosyal ağları kullanırken, genellikle gizli kimliklerin tuzaklarının farkında değildirler. Sanal davranışın çevrimdışı temasa geçebileceği, çocuk tacizi ve istismarı, pedofili, çocukların cinsel maksatla suça teşviki ve hatta çocuk kaçakçılığı riskini artıran maskeli kimlik, istismarcılar tarafından sıklıkla kullanılan bir yaklaşımdır.

Genellikle mevzuatta “çocuk pornografisi”¹⁰³ olarak adlandırılan çocuklara yönelik cinsel istismar görüntüleri tipik olarak gerçek dünyadaki cinsel saldırıların dijital temsildir. Araştırmalar, çevrimiçi çocuklara yönelik cinsel istismar içeriğinin mağdurlarının genellikle çok genç olduğunu ve istismarın şiddetli ve insanlık dışı olduğunu göstermektedir.

Çevrimiçi olarak paylaşılmakta olan çocuk cinsel istismar içeriğinin gerçek miktarının belirlenmesi zor olsa da, içeriğin çoğu, arama motorları tarafından normalde alınmayan “derin ağ” da bulunur. Birçok suçlu daha güvenli olmaya ve derinlemesine teknik bilgi edinmeye başladıkça, Darknet avcı ve sübyancılar arasında çok popüler hale gelmektedir.

İnternette açık bir şekilde dolaşan neredeyse tüm çocuk cinsel istismarı içeriği eski içeriğin yeniden dolaştırılmasından ibarettir; yeni içerik genellikle yeni bir kurbanın olduğunu gösterir. Çocuğa cinsel istismara uğradığını gösteren içerik çevrimiçi olarak keşfedildiğinde, iki açık

öncelik vardır: içeriği kamuoyundan kaldırmak ve kötüye kullanılan mağdurları bulmak. Daha sonra mağdur zarar görmeden uzaklaştırılabilir ve uygun destek önerilebilir.

Zorlukları ele almak

Çevrimiçi riskler söz konusu olduğunda, uygun mevzuat ile politikayı (mevzuat, öz düzenleme ve eş düzenleme ve diğer politika önlemleri dahil) bir araya getiren bir yaklaşımın yanı sıra teknik araçlar, eğitim ve farkındalık da geniş bir yoldaki risklerin üstesinden gelmek için kullanılabilir.

Yasal önlemler

Normatif bir bakış açısına göre, birçok ülke, tanım ve yorumlar ülkeden ülkeye değişebilse de, belirli içeriği yasa dışı kılan kanunları yürürlüğe koymuştur. Uluslararası düzeyde, kilit araçlar **BM Çocuk Hakları Sözleşmesi** ve **çocuk satışı, çocuk fuhuşu ve çocuk pornografisi ile ilgili İkinci İsteğe Bağlı Protokol**; **CoE Siber Suçlar Sözleşmesi** ve **Çocukların Cinsel Sömürüye ve Cinsel İstismara Karşı Korunmasına İlişkin Sözleşme** (Lanzarote Sözleşmesi olarak da bilinir) olarak bahsedilebilir. Uluslararası Kayıp ve İstismara Uğrayan Çocuklar Merkezi (ICMEC), ulusal mevzuatı değerlendirme çerçevesini geliştirmiş ve ülkeler arasındaki mevzuatı gözden geçirmek için düzenli olarak kullanmaktadır.

Kendiliğinden ve işbirliğine dayanan önlemler

Öz düzenleme (sektörün gönüllü anlaşması) ve eş düzenlemenin (hükümet ve özel düzenlemelerin birleşimi) etkili yaklaşımlar olduğu özellikle endüstri tarafından tespit edilmiştir. Örneğin, ISS'ler gönüllü olarak bildirimde bulunmak için aşağı doğru önlemleri alabilirler ve ayrıca belirli yasadışı içerik türlerini filtreleyebilirler; Sosyal medya platformları çocuklar için minimum yaş gereksinimlerini belirleyebilir. Açıkça tanımlanmış süreçler ve protokollerle endüstri ve emniyet teşkilatı arasındaki iyi işleyen bir ilişki, birlikte çalışmak için önemlidir. 2008'de CoE, **kolluk kuvvetleri ve ISS'ler arasında siber suçlara karşı işbirliği için Kılavuzlar** yayınlanmıştır.¹⁰⁴

Teknik önlemler

Diğer tekniklerle birlikte kullanılması gereken çeşitli teknik ve sürece dayalı önlemler, çocuğun cinsel istismarı ile mücadele edebilir. Acil yardım hattı raporlama mekanizmaları ve bildirim geri alma istekleri sıklıkla birlikte çalışır. 45 ülkede (şu ana kadar) 51 çağrı hattından oluşan ortak bir çalışma ağı olan Uluslararası İnternet Yardım Hatları Birliği (INHOPE), çoğu kez bir gün içinde yasa uygulayıcı kurumlara iletilen yıllık binlerce rapor işlemektedir. Diğer teknik önlemler arasında mağdur tespit veritabanlarının korunması ve belirli sitelere erişimin engellenmesi ve soruşturmaya yardımcı olmak için dijital parmak izi, veri madenciliği ve analitik kullanımı yer almaktadır.

Farkındalığı artırma ve eğitim

Çocukları, gençleri, ebeveynleri, velileri ve eğitimcileri hedef alan birçok kampanya ulusal, bölgesel ve uluslararası düzeyde gerçekleştirilmektedir. İnternette bir farkındalığı arttırma kaynakları da mevcuttur. ITU'nün Çocuk Çevrimiçi Koruma (COP) girişimi, çocuklar, ebeveynler ve veliler, eğitimciler, sektörler ve politika yapıcılar için yönergeler sunmaktadır.¹⁰⁵ 31 ulusal farkındalık merkezi olan bir Avrupa ağı olan Daha Güvenli İnternet Merkezleri Ağı (INSAFE), ailelere farklı dillerde araçlar sağlamaktadır. Her şubat ayında çeşitli ülkelerde kutlanan Daha Güvenli İnternet Günü, İnternet'in özellikle dünya genelinde çocuklar ve gençler arasında daha güvenli kullanılmasını teşvik etmeyi amaçlamaktadır.

Eşgüdümlü yaklaşım

Çocuğun çevrimiçi korunması ve çocukların çevrimiçi cinsel istismarı ve sömürüsü ile mücadele, aynı zamanda etkili ve koordineli bir şekilde birlikte hareket etmesi gereken paydaşların çabalarını da gerektirir. Ebeveynler ve eğitimciler, çocukları yönlendirmek ve desteklemekle yükümlüdür ve eğitimin ve farkındalığın önemli bir birinci savunma hattı olduğu kabul edilir. Hükümetlerin çocukları korumak için birincil sorumluluğu vardır ve birçok ülkede çocuğun çevrimiçi korunması ulusal politika gündeminde üst sıralardadır. Kolluk kuvvetleri, interneti suçlulardan daha güvenli hale getirmede önemli bir rol oynamaktadır ve ayrıca çevrimiçi çocuk cinsel istismarı ile mücadele etmek için bölgesel ve uluslararası seviyelerde çalışmaktadır. Hem Avrupa Polis Ofisi (Europol) hem de Uluslararası Ceza Polis Teşkilatı (INTERPOL), cinsel istismar mağdurlarının tespitine yardımcı olan çeşitli veritabanları işletmektedir.

Endüstri, çevrimiçi ortamın güvenli ve emniyetli olmasını sağlama sorumluluğuna sahiptir. Servis sağlayıcılar böyle bir ortam yaratmada kilit bir rol oynayabilir ve filtreler ve raporlama mekanizmaları gibi birçok araç bu amaçla kullanılabilir. Endüstri koalisyonları arasında Teknoloji Koalisyonu; ABD'de Çocuk Pornografisine Karşı Mali Koalisyon, Asya Pasifik Mali Koalisyonu ve Avrupa Mali Koalisyonu dahil finansal koalisyonlar; ve Çocuk Cinsel İstismarı İçeriğine Karşı Küresel GSMA Mobil İttifakı gibi koalisyonları kapsamaktadır.

Alanında uzman olan birçok profesyonelin bilgi ve tecrübe ile paha biçilmez girdi sağlayabilecek sivil toplum kuruluşlarında aktif olmaları muhtemeldir. Ulusal STK'lar, ECPAT International ve ICMEC gibi uluslararası ağlar aracılığıyla işbirliği yapabilir. Bazı bölgesel girişimler ve organizasyonlar da çevrimiçi çocuk güvenliğine odaklanmaktadır.

Çocuk STK'ları ve çocuk yardım hatları aynı zamanda çocuk cinsel istismarına ve sömürüsüne karşı mücadelede (hem çevrimiçi hem de çevrimdışı) kilit paydaşlardır ve sorunun boyutunu ve doğasını anlamada ve aynı zamanda istismar mağdurlarına danışmanlık ve destek sağlamada değerli ortaklardır.

www.igbook.info/childsafety

Sonnotlar

- 1 Radunović V (2013) DDoS – Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR), 26–28 Kasım, Belgrade, Serbia, pp. 5–9.
- 2 Goodin D (2015) Botnet that enslaved 770,000 PCs worldwide comes crashing down. Ar- stechnica, 13 April. <http://arstechnica.com/security/2015/04/botnet-that-en- slaved-770000-pcs-worldwi- de-comes-crashing-down/> [Erişim 21 Ekim 2016].
- 3 United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of In- formation and Telecommunications in the Context of International Security. http://www.un.org/ga/ search/view_doc.asp?symbol=A/RES/53/70 [Erişim 8 Şubat 2016].
- 4 United Nations (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Erişim 6 Haziran 2016].
- 5 Grigsby A (2015) The UN GGE on cybersecurity: What is the UN's role? Council on Foreign Relations Blog, 15 April. <http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cy- bersecurity-w- hat-is-the-uns-role/> [Erişim 8 Şubat 2016].
- 6 ITU (no date) Global Cybersecurity Agenda. <http://www.itu.int/osg/csd/cybersecu- rity/gca/> [Erişim 22 Ekim 2016].
- 7 ITU (no date) Global Cybersecurity Index. <http://www.itu.int/en/ITU-D/Cyberse- curity/Pages/ GCI.aspx> [Erişim 22 Ekim 2016].
- 8 DiploFoundation (2015) IGF Summary. Just-in-time Reporting from the 2015 Internet Governance Forum. <http://digitalwatch.giplatform.org/sites/default/files/IGFReportWEB. pdf> [Erişim 8 Şubat 2016].
- 9 Hague W (2011) London Conference on Cyberspace – Chairman's Summary. http://www.gccs2015.com/sites/default/files/documents/London%20Conference%20on%20Cy- berspace%20 -%20Chair's%20Summary%20-%20201-2%20Nov%202011%20_1_.pdf [Erişim 8 Şubat 2016].
- 10 Global Forum on Cyber Expertise (2015) The Hague Declaration on the GFCE. <https://www.the- gfce.com/documents/publications/2015/04/16/the-hague-declaration-on-the- gfce> [Erişim 22 Ekim 2016].
- 11 Statement by NATO Secretary General following the North Atlantic Council meeting at the level of NATO Defence Minister. [http://www.nato.int/cps/en/natohq/opinions_132349. htm?selectedLoca- le=en](http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLoca- le=en) [Erişim 12 Ağustos 2016].
- 12 NATO Cooperative Cyber Defence Centre of Excellence (2013) Tallinn Manual on the Interna- tional Law Applicable to Cyber Warfare. <https://ccdcoe.org/research.html> [Erişim 22 Ekim 2016].
- 13 Klimburg A (Ed.) (2012) National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence Publication. <https://ccdcoe.org/publications/ books/NationalCyberSe- curityFrameworkManual.pdf> [Erişim 22 Ekim 2016].
- 14 Council of Europe (2001) Convention on Cybercrime. <http://conventions.coe.int/ Treaty/en/Trea- ties/Html/185.htm> [Erişim 21 Ekim 2016].
- 15 European Union (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Se- cure Cyberspace. <https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-open-safe-and-secure-cyberspace> [Erişim 22 Ekim 2016].
- 16 European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Coun- cil of 6 Temmuz 2016 concerning measures for a high common level of security of network and

- information systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TX/T/?uri=uriser-v%3A0J.L_.2016.194.01.0001.01.ENG [Erişim 18 Ağustos 2016].
- 17 OSCE (2013) Decision No. 1106 Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. <http://www.osce.org/pc/109168?download=true> [Erişim 22 Ekim 2016].
 - 18 OSCE (2016) Decision No. 1202 OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. <http://www.osce.org/pc/227281?download=true> [Erişim 22 Ekim 2016].
 - 19 Organization of American States General Assembly (2003) Resolution AG/RES.1939 (XXXI-II-O/03). Development of an Inter-American Strategy to Combat Threats to Cybersecurity. http://www.oas.org/juridico/english/agres_1939.pdf [Erişim 22 Ekim 2016].
 - 20 Organization of American States (2011) Inter-American Cooperation Portal on Cyber-crime. <http://www.oas.org/juridico/english/cyber.htm> [Erişim 8 Şubat 2016].
 - 21 ASEAN Regional Forum (2012) Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security. <https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARF-statementCS.pdf> [Erişim 8 Şubat 2016].
 - 22 ASEAN (2014) ASEAN's Cyber Confidence Building Measures. Presentation by the ASEAN Secretariat. UNIDIR Cyber Stability Seminar 'Preventing Cyber Conflict', 10 Şubat 2014, Geneva, Switzerland. <http://www.unidir.ch/files/conferences/pdfs/the-asean-s-cyber-confidence-building-measures-en-1-958.pdf> [Erişim 8 Şubat 2016].
 - 23 Grigsby A (2015) Will China and Russia's updated code of conduct get more traction in a post-Snowden era? Council on Foreign Relations blog, 28 January. <http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/> [Erişim 22 Ekim 2016].
 - 24 African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. <http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> [Erişim 6 Haziran 2016].
 - 25 Microsoft (2015) International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CF-C36FD44/International_Cybersecurity_%20Norms.pdf [Erişim 8 Şubat 2016].
 - 26 Politika üçgenindeki etkileşimin derin analizi için 2015 IGF Çalıştayının raporuna bkz: Cybersecurity, human rights and Internet business triangle. <http://digitalwatch.giplatform.org/sessions/cybersecurity-human-rights-and-internet-business-triangle> [Erişim 6 Haziran 2016].
 - 27 Domain Name System Security Extensions explained. <http://everything.explained.at/DNSSEC/> [Erişim 21 Ekim 2016].
 - 28 Radunović V (2013) Waging a (private) cyber war. <https://www.diplomacy.edu/blog/waging-private-cyberwar> [Erişim 22 Ekim 2016].
 - 29 Perlroth N and Gellese D (2014) Russian gang said to amass more than a billion stolen Internet credentials. New York Times, 5 August. <http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html> [Erişim 22 Ekim 2016].
 - 30 RT (2014) Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. 24 Şubat. <https://www.rt.com/news/brazil-eu-cable-spying-504/> [Erişim 22 Ekim 2016].
 - 31 Keck Z (2014) China expands cyber spying. The Diplomat, 12 April. <http://thediplomat.com/2014/04/china-expands-cyber-spying/> [Erişim 22 Ekim 2016].

- 32 Ranger S (2014) We're the real hacking victims, says China. ZDNet, 20 May. [http:// www.zdnet.com/article/were-the-real-hacking-victims-says-china/](http://www.zdnet.com/article/were-the-real-hacking-victims-says-china/) [Erişim 22 Ekim 2016].
- 33 Spetalnick M and Martina M (2015) Obama announces 'understanding' with China's Xi on cyber theft but remains wary. Reuters, 26 September. <http://www.reuters.com/article/us-usa-china-idUSKCN0RO2HQ20150926> [Erişim 8 Şubat 2016].
- 34 G20 (2015) G20 Leaders' Communiqué. Antalya Summit, 15–16 Kasım 2015. <http://g20.org/English/Documents/PastPresidency/201512/P020151228335504307519.pdf> [Erişim 8 Şubat 2016].
- 35 Schneier B (2013) NSA surveillance: A guide to staying secure. The Guardian, 6 September. <https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance> [Erişim 22 Ekim 2016].
- 36 For a listing of anti-cybercrime networks, organisations and initiatives worldwide, refer to the CoE's resources page. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp [Erişim 22 Ekim 2016].
- 37 The Commonwealth (no date) Commonwealth Cybercrime Initiative. [http:// thecommonwealth.org/commonwealth-cybercrime-initiative](http://thecommonwealth.org/commonwealth-cybercrime-initiative) [Erişim 22 Ekim 2016].
- 38 Bailey C (2002) The International Convention on Cybercrime. Association for Progressive Communications. http://rights.apc.org/privacy/treaties_icc_bailey.shtml [Erişim 7 March 2016].
- 39 Council of Europe (2014) Recommendation CM/Rec (2014) 6 of the Committee of Ministers to member states on a Guide to human rights for Internet users. [https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31) [Erişim 20 Ekim 2016].
- 40 European Union (2006) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. [http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF) [Erişim 22 Ekim 2016].
- 41 For a detailed overview of the data retention issues in EU, refer to European Commission (2011) Evaluation report on the Data Retention Directive (Directive 2006/24/EC). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF> [Erişim 22 Ekim 2016].
- 42 CJEU (2014) Judgement of the Court in Joined Cases C-293/12 and C-594/12: Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&d oclang=EN&mode=lst&dir=&occ=first&part=1&cid=106306> [Erişim 22 Ekim 2016].
- 43 European Commission (2004) Critical Infrastructure Protection in the Fight Against Terrorism. Communication from the Commission to the Council and the European Parliament. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702> [Erişim 22 Oc tober 2016].
- 44 Essers L (2014) Cyberattack on German steel factory causes 'massive damage'. IT World, 19 December. <http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html> [Erişim 22 Ekim 2016].
- 45 IETF (2007) Internet Security Glossary, Version 2. [https://tools.ietf.org/html/ rfc4949](https://tools.ietf.org/html/rfc4949) [Erişim 18 Ağustos 2016].
- 46 USA White House (2013) Presidential Policy Directive – Critical Infrastructure Security and Resilience. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> [Erişim 18 Ağustos 2016].
- 47 European Commission (2006) European Programme for Critical Infrastructure Protection. Available

- at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A133260> [Erişim 18 Ağustos 2016].
- 48 European Union (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF> [Erişim 18 Ağustos 2016].
- 49 OECD (2008) Recommendation of the Council on the Protection of Critical Information Infrastructures. <http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117&Lang=en&Book=> [Erişim 22 Ekim 2016].
- 50 The Cyberterrorism Project (2013) What is cyberterrorism? UK Legal Definition. <http://www.cyberterrorism-project.org/what-is-cyberterrorism> [Erişim 22 Ekim 2016].
- 51 Krasavin S (2009) What is Cyber-terrorism? Computer Crime Research Center. <http://www.crime-research.org/library/Cyber-terrorism.htm> [Erişim 22 Ekim 2016].
- 52 Denning D (2000) Statement. http://fas.org/irp/congress/2000_hr/00-05-23denning.htm [Erişim 22 Ekim 2016].
- 53 Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China, 18 April 2016. http://mea.gov.in/bilateral-documents.htm?dtl/26628/Joint_Communique_of_the_14th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China [Erişim 22 Ekim 2016].
- 54 UN News Centre (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 May. <http://www.un.org/apps/news/story.asp?NewsID=53909#.WAsjTeZlqZ> [Erişim 22 Ekim 2016].
- 55 G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. <http://www.mofa.go.jp/files/000160278.pdf> [Erişim 22 Ekim 2016].
- 56 Microsoft (2016) Microsoft's approach to terrorist content online. <http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.00001i30hhw72cdzpxr8cky3uuvbs> [Erişim 22 Ekim 2016].
- 57 Greenberg A (2016) Google's clever plan to stop aspiring ISIS recruits. Wired, 17 September. <https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/> [Erişim 22 Ekim 2016].
- 58 UN News Centre (2016) UN expert warns combat against violent extremism could be used as 'excuse' to curb free speech. 3 May. <http://www.un.org/apps/news/story.asp?NewsID=53841#.WAs1FjeZlqb> [Erişim 22 Ekim 2016].
- 59 GCN (2012) DOD wants cyberterrorism-prediction software. 31 Temmuz. <http://gcn.com/articles/2012/07/31/agg-dod-small-biz-software-support.aspx> [Erişim 22 Ekim 2016].
- 60 The Clean IT Project (2012) About the project. <http://www.cleanitproject.eu/about-the-project/> [Erişim 18 Ağustos 2016].
- 61 United Nations General Assembly (2006) Resolution A/60/288. The United Nations Global Counter-Terrorism Strategy. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288 [Erişim 22 Ekim 2016].
- 62 UNODC (2012) The use of the Internet for terrorist purposes. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Erişim 22 Ekim 2016].
- 63 UN Security Council Counter-Terrorism Committee (2015) Special Meeting of the Counter-Terrorism Committee and technical sessions of the Counter-Terrorism Committee Executive Directorate

- on preventing and combating abuse of ICT for terrorist purposes. http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html [Erişim 22 Ekim 2016].
- 64 Berenger RD (2012) *Cyber Warfare*. In Yan Z [ed] *Encyclopedia of Cyber Behavior*. Hershey, PA: Information Science Reference, pp. 1074–1087.
- 65 BBC News (2007) Estonia hit by ‘Moscow cyber war’. 17 May. <http://news.bbc.co.uk/2/hi/europe/6665145.stm> [Erişim 22 Ekim 2016].
- 66 Swaine J (2008) Georgia: Russia ‘conducting cyber war’. *The Telegraph*, 11 Ağustos. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [Erişim 22 Ekim 2016].
- 67 Sanger D (2012) Obama sped up wave of cyberattacks against Iran. *New York Times*, 1 Haziran. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> [Erişim 22 Ekim 2016].
- 68 Nakashima E (2012) Iran blamed for cyberattacks on U.S. banks and companies. *The Washington Post*, 21 September. https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html [Erişim 22 Ekim 2016].
- 69 Lee C and Solomon J (2015) US targets North Korea in retaliation for Sony hack. *The Wall Street Journal*, 3 January. <http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942> [Erişim 22 Ekim 2016].
- 70 Foster P (2013) China denies Pentagon cyber-attack claims. *The Telegraph*, 7 May. <http://www.telegraph.co.uk/news/worldnews/asia/china/10040757/China-denies-Pentagon-cyber-attack-claims.html> [Erişim 22 Ekim 2016].
- 71 Ranger S (2014) We’re the real hacking victims, says China. *ZDNet*, 20 May. <http://www.zdnet.com/article/were-the-real-hacking-victims-says-china/> [Erişim 22 Ekim 2016].
- 72 Munich Security Conference (2015) *Collapsing Order, Reluctant Guardians? Munich Security Report 2015*. Munich Security Conference. <https://www.securityconference.de/en/activities/munich-security-report/> [Erişim 22 Ekim 2016].
- 73 Radunović V (2013) DDoS – Available Weapon of Mass Disruption. *Proceedings of the 21st Telecommunications Forum (TELFOR)*, 26–28 Kasım, Belgrade, Serbia, pp. 5–9.
- 74 Appelbaum et al. (2014) *Prying Eyes: Inside the NSA’s War on Internet Security*. *Der Spiegel*, 28 December. <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html> [Erişim 11 Ağustos 2016].
- 75 The Wassenaar Arrangement. <http://www.wassenaar.org/> [Erişim 22 Ekim 2016].
- 76 Clipper yaklaşımı 1993 yılında ABD hükümeti tarafından önerildi. Özünde, tüm telefonlarda ve diğer sesli iletişim araçlarında kullanılması öngörülen bir Clipper yongası kullanılıyordu. Clipper çipinin, hükümetler tarafından yasal gözetim için kullanılabilecek bir ‘arka kapısı’ vardı. ABD hükümeti, insan hakları savunucuları ve halkın güçlü muhalefetinden sonra 1995’te bu teklifi bıraktı. Denning D (1995) *The case for clipper*. *MIT Technology Review*. MIT: Cambridge, MA, USA. http://encryption_policies.tripod.com/us/denning_0795_clipper.htm [Erişim 22 Ekim 2016].
- 77 Huggler J (2015) Man arrested in Germany on suspicion of illegal arm dealing in terror crack-down. *The Telegraph*, 27 Kasım. <http://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html> [Erişim 11 Ağustos 2016].
- 78 Berkman Üniversitesi İnternet ve Toplum Merkezi tarafından Harvard Üniversitesi’nde yayınlanan bir araştırma, “karanlık” metaforunun, ‘hükümetin şüpheli teröristlerin ve suçluların iletişimine erişme kapasitelerinin geleceğini tam olarak tarif etmediğini savunmaktadır. Şifreleme teknolojilerinin mev-

cudiyetinin artması kesinlikle belirli koşullar altında devlet gözetimini engellemektedir ve bu anlamda hükümet bazı gözetim olanaklarını yitirmektedir. Bununla birlikte, [...] teknolojik gelişmelerin ve piyasa güçlerinin bir araya gelmesi, bu boşlukların bir kısmını doldurması ve daha geniş bir şekilde hükümetin gözetimden kritik bilgi toplamak için yeni fırsatlar kazanması muhtemeldir. Daha fazla bilgi için bkz. The Berkman Center for Internet and Society at Harvard University (2016). Don't Panic. Making Progress on the 'Going Dark' Debate. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Pan-ic_Making_Progress_on_Going_Dark_Debate.pdf [Erişim 12 Temmuz 2016].

- 79 55 ülkeden 865 donanım veya yazılım ürünü şifrelemesini inceleyen bir araştırma, bu tür ürünlerin geniş mevcudiyetinden dolayı, kolluk kuvvetleri tarafından istenen zorunlu arka kapıların 'etkisiz' olacağına işaret ediyor. Bunun nedeni, şifreleme ürünleri pazarının uluslararası olduğu ve suçluların belirli bir ülkede ulusal mevzuat kapsamına girmeyen ürünlere geçebileceği göz önüne alındığında, bu tür arka kapıların kolayca kaldırılmasıdır. Bunun yerine, arka kapıyı zorunlu kılan herhangi bir ulusal yasa, "bu ürünlerin masum kullanıcılarını" etkileyecek, ilgili ülkedeki insanları "siber suçlular ve diğer hükümetler tarafından arka kapı kullanımına açık" olarak bırakacaktır. Daha fazla bilgi için bkz. Schneier B, Seidel K and Vijayakumar S (2016) A Worldwide Survey of Encryption Products. <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf> [Erişim 12 Temmuz 2016].
- 80 Rapor için bkz. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 [Erişim 12 Temmuz 2016].
- 81 DiploFoundation (2016) Apple vs FBI: A Socratic dialogue on privacy and security DiploFoundation blog 22 March. <https://www.diplomacy.edu/blog/apple-vs-fbi-socratic-dialogue-privacy-and-security> [Erişim 11 Ağustos 2016].
- 82 Dridex'in mali Trojan'ı 2016'da ciddi endişelere neden oldu; siber güvenlik şirketleri 'tüketicilerin ve işletmelerin karşılaştığı en ciddi çevrimiçi tehditlerden biri' olarak nitelendirdi. Büyük spam kampanyalarıyla dağıtılan Trojan, dünyadaki yüzlerce bankanın ve diğer finans kurumlarının müşterilerinden bankacılık kimlik bilgileri toplama yeteneğine sahiptir. Daha fazla bilgi için bkz: O'Brien D (2016) Dridex: Tidal waves of spam pushing dangerous financial Trojan. Symantec. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf [Erişim 14 Temmuz 2016].
- 83 Trustwave (2016) Global Security Report. <https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/> [Erişim 13 Temmuz 2016].
- 84 Gudkova D et al. (2016) Spam and phishing in Q1 2016. Kaspersky Lab. <https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/> [Erişim 13 Temmuz 2016].
- 85 Locky'nin çalışma şekli basit: kullanıcılar spam e-postalarıyla gönderilen kötü amaçlı ekleri açmak için kandırılıyor. Kullanıcıların cihazlarına yüklendikten sonra, Trojan tüm verileri şifreler ve kullanıcıdan şifrelerin çözülmesi için kullanıcıdan bir fidye ödemesi istenir. Daha fazla bilgi için bkz: Sinityn F (2016) Locky: the encryptor taking the world by storm. Kaspersky Lab. <https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/> [Erişim 14 Temmuz 2016].
- 86 More references to Can-Spam are the Bureau of Consumer Protection (2009). The CAN-SPAM Act: A Compliance Guide for Business. <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business> [Erişim 22 Ekim 2016].
- 87 Haziran 2016'da, bir ABD vatandaşı iki buçuk yıl hapis cezasına çarptırıldı ve Facebook kullanıcılarına 27 milyondan fazla spam mesajı gönderdiği için 310.628.55 USD tazminat ödemesi istendi. ABD'nin Kuzey Bölgesi Federal Başsavcılığı'na göre, adam yasal olarak Facebook kullanıcı hesaplarının bilgilerini elde etti, sakladı ve kullandı ve kullanıcıları diğer web sitelerine yönlendirerek para kazandı. Kasım 2008 ile Mart 2009 arasında yürütülen plan, yaklaşık 500.000 meşru Facebook he-

- şabını riske attı. Daha fazla bilgi için bkz. the press release from the Office of the US Attorney for the Northern District of California. <https://www.justice.gov/usao-ndca/pr/sanford-spam-king-wal-lace-sen-tenced-two-and-half-years-custody-spamming-facebook-users> [Erişim 13 Temmuz 2016].
- 88 European Union (2012) Directive 2002/58/EC of the European Parliament and of the Council of 12 Temmuz 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058> [Erişim 22 Ekim 2016].
- 89 BBC NEWS (2004) European anti-spam laws lack bite. 28 April. <http://news.bbc.co.uk/2/hi/technology/3666585.stm> [Erişim 6 Ekim 2016].
- 90 New Zealand Law Society (2016) NZ signatory to international anti-spam MOU. 15 Haziran. Available at <https://www.lawsociety.org.nz/news-and-communications/latest-news/news/nz-signatory-to-international-anti-spam-mou> [Erişim 22 Ekim 2016].
- 91 ITU (2012) Resolution 52 of the World Telecommunication Standardization Assembly: Countering and combating spam. <https://ccdcoc.org/sites/default/files/documents/ITU-121129-CombSpamWTSARes52.pdf> [Erişim 22 Ekim 2016].
- 92 APEC (2012) APEC Principles for Action against Spam. http://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel/annex_e.aspx [Erişim 22 Ekim 2016].
- 93 African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf [Erişim 22 Ekim 2016].
- 94 Spam etkinleştirme yapan ülkeler hakkındaki güncel istatistikler Spamhaus Project tarafından sağlanmaktadır. Bkz. <https://www.spamhaus.org/statistics/countries/> [Erişim 14 Temmuz 2016]. Spamhaus ayrıca, spam destekleyen ISS'ler, en kötü spam gönderenler, tespit edilen en yüksek spam countries botları sayısı, spam'lerden en çok zarar görmüş TLD'ler, vb. istatistik bilgileri sağlamaktadır.
- 95 Elektronik kayıtların kriptografik algoritmalar kullanılarak doğrulanması ve belgelenmesi; 'Elektronik imzalar', dijital imzalar ve biyometri gibi daha geniş bir onaylama teknikleri yelpazesi içeren daha geniş bir terimdir.
- 96 EU Kids Online (2014) EU Kids Online: Findings, Methods, Recommendations. London: LSE. <http://eprints.lse.ac.uk/60512/> [Erişim 9 Ağustos 2016].
- 97 For a more detailed explanation of these three approaches, consult: ILPF (1999) Survey of International Electronic and Digital Signature Initiatives. <http://www.ilpf.org/groups/survey.htm#IB> [Erişim 21 Ağustos 2016].
- 98 European Union (2014) Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG [Erişim 12 Ağustos 2016].
- 99 UNCITRAL (2001) Model Law on Electronic Signatures. http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [Erişim 22 Ekim 2016].
- 100 Longmuir G (2000) Privacy and Digital Authentication. www.longmuir.net/papers/Research%20Paper.doc [Erişim 20 Ağustos 2016]. Bu makale dijital dünyada kimlik doğrulama ihtiyacının kişisel, topluluk ve devlet yönlerine odaklanmaktadır.
- 101 Yasal araçlara ve uluslararası uygulamalara uygun olarak, bir "çocuğun", 18 yaşın altındaki herhangi bir insanı ifade ettiği anlaşılmaktadır.
- 102 Typologies include Barbosa A et al. (2013) Risks and Safety on the Internet: Comparing Brazilian and European Results. London: LSE. <http://eprints.lse.ac.uk/54801/> [Erişim 9 Ağustos 2016];

- OECD (2012) The Protection of Children Online; Recommendation of the OECD Council. http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [ac- cessed 9Ağustos 2016].
- 103 “Çocuk pornografisi” terimi, genellikle yetişkinlerin rızası arasındaki cinsel aktivite tasviri ile ilişkili olduğu için bir sorun teşkil eder. Terimler küfürlü ve sömürücü yönleri vurgulayamadığından, “çocuk cinsel istismar materyali” ve “çocuk cinsel sömürü materyali” dahil olmak üzere daha fazla tercih edilen terminoloji lehine giderek daha fazla kaçınılmaktadır. Interagency Working Group on Sexual Exploitation of Children (2016) Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. [http://www.ilo.org/ipec/ Informationresources/WCMS_490167/ lang--en/index.htm](http://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm) [Erişim 12 Ağustos 2016].
- 104 Council of Europe (2008) Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime. [https://rm.coe.int/CoERMPublicCommon- SearchServices/ DisplayDCTMContent?documentId=09000016802fa3ba](https://rm.coe.int/CoERMPublicCommon-SearchServices/DisplayDCTMContent?documentId=09000016802fa3ba) [Erişim 22 Ekim 2016].
- 105 ITU (no date) Guidelines for Child Online Protection. [http://www.itu.int/en/cop/ Pages/guidelines.aspx](http://www.itu.int/en/cop/Pages/guidelines.aspx) [Erişim 22 Ekim 2016].

The background is a solid teal color. It features several large, semi-transparent geometric shapes: a large downward-pointing triangle at the top left, a smaller downward-pointing triangle at the top right, a circular shape with diagonal lines on the right side, and several upward-pointing triangles at the bottom. The text is centered in the middle of the page.

Bölüm 4

Yasal sepet

YASAL SEPET

Yasanın temel sosyal işlevleri, atalarımızın insan toplumunu örgütlemek için kurallar kullanmaya başladıkları, binlerce yıl öncesindeki gibi İnternet çağında da mevcuttur. Hukuk, şirketlerden ulusal devletlere kadar bireyler ve kurdukları kurumlar arasındaki hak ve sorumlulukları düzenlemektir. İnternetin sosyal iletişim aracı ve ekonomik kalkınmanın itici gücü olarak daha fazla büyümesi bakımından hukukun üstünlüğü ve yasal güvenlik esastır.

İnternetin yasal olarak düzenlenmesi, siber hukuktan gerçek hukuk yaklaşımına doğru gelişmiştir. İnternetin ilk günlerinde, İnternet'in siber alanda yeni türden sosyal ilişkiler ortaya koyduğu varsayımına dayanarak siber hukuk yaklaşımı öndeydi. Sonuç olarak, siber alanın düzenlenmesi için yeni siber kanunların formüle edilmesine ihtiyaç vardı. Bu yaklaşım için bir argüman, İnternetin sınır ötesi iletişimini kolaylaştıran hızının ve hacminin mevcut yasal kuralların uygulanmasını engelleyeceği yönünde idi. Bir başka sık tartışılan tartışma, geleneksel düzenlemenin (örneğin suç, vergilendirme ile ilgili) yeterince etkili olmayacağıydı.¹ Bununla birlikte, yasaların yasaklanmış davranışları imkansız kılmadığını, sadece cezalandırılabilir olduğunu unutmamak önemlidir.

Ancak daha yakın zamanlarda İnternet'in sosyal hayata yaygınlaştırılmasıyla birlikte gerçek hukuk yaklaşımı öne çıkmıştır. Bu yaklaşıma göre, internet, duman sinyallerinden telefona kadar uzun bir evrede, önceki telekomünikasyon teknolojilerinden farklı olarak ele alınmamaktadır. Sonuç olarak, mevcut yasal kurallar İnternete de uygulanabilir. Örneğin, BM GGE'nin 2013 raporunda, mevcut uluslararası hukukun devletlerin ICT kullanımı için geçerli olduğunu yineledi.² Bu sonuç, daha sonra WSIS + 10 inceleme sürecinde UNGA tarafından memnuniyetle karşılandı.³ İnsan hakları alanında, UNGA ve UNHRC kararları, insanların çevrimdışı olarak kullandıkları insan haklarının da çevrimiçi olarak da korunması gerektiği ilkesini kesin olarak belirlemiştir.⁴

Var olan yasanın internete uygulanabilir olup olmadığı sorusunun cevabı olumlu olsa da, geriye kalan asıl soru mevcut kuralların nasıl uygulanacağıdır. Örneğin, önemli bir zorluk, İnternet ile ilgili uluslararası unsurları içeren durumlarda yasal tazminatın sağlanmasıdır. Bireyler ve şirketler uluslararası özel hukuka güvenebilirken, ulusal hükümetler uluslararası kamu hukuku mekanizmalarını kullanabilir. Her iki yaklaşım da uzun bir geleneğe sahiptir ve esasında ulusal sınırların ötesinde alışverişlerin daha az yoğun dönemde geliştirilmiştir. Bu yaklaşımlar incelenmeli ve ihtiyaç duyduğumuzda internet meselelerinde dünya çapında bireylere kurumlara adalet sağlamak yönünde geliştirilmelidir.

Yasal enstrümanlar

İnternet alanında halihazırda uygulanmış veya uygulanabilecek çok çeşitli yasal araçlar bulunmaktadır. Bunlar ulusal düzeyde ve uluslararası düzeyde geçerli araçlar olarak sınıflandırılmaktadır.

Ulusal yasal araçlar, sosyal normlar, ve öz-düzenleme

İnternet ile ilgili yasal düzenlemelerin çoğu ulusal düzeydedir. Bu, internet iletişiminin sınır

ötesi doğası ile birlikte kaçınılmaz bir gerilim yaratmaktadır. Unutulma hakkı durumunda olduğu gibi, bazı mahkeme kararlarının kendi yetki alanlarının ötesinde daha geniş bir etkisi vardır. Vatandaşların ve şirketlerin, internet üzerindeki yasal haklarını ve menfaatlerini korumak için (AB durumunda, uluslararası CJEU’da istisnası ile) ulusal mahkemeleri kullanmaları beklenmektedir.

Yasama

Yasama faaliyetleri İnternet alanında giderek artan bir biçimde yoğunlaşmıştır. Bu, özellikle İnternet’in yaygın olarak kullanıldığı ve ekonomik ve sosyal ilişkiler üzerinde yüksek derecede etkisi olan ülkelerdeki durumdur. Bugüne kadar, İnternet mevzuatı için öncelikli alanlar gizlilik ve veri koruması, fikri mülkiyet, vergi ve siber suçlar olmuştur.

Teknolojik alanda sürekli ilerleme, teknoloji ile ilgili konulara değinen mevzuatın oluştuğunda izlenecek olan teknolojik tarafsızlık ilkesinin benimsenmesine de yol açmıştır. Uygulamada, bu ilke, yasanın belirli teknolojilere açıkça atıfta bulunmaması veya bir teknolojiyi diğerine tercih etmemesi gerektiği anlamına gelir; kanunun tarafsız kalmasını sağlayacak genel terimler kullanılmalıdır.

Ancak, sosyal ilişkiler sadece yasa koyucular tarafından düzenlenemeyecek kadar karmaşıktır. Toplum dinamikler ve mevzuat her zaman toplumsal değişimin gerisinde kalmaktadır. Bu, teknolojik gelişmelerin sosyal gerçekliği yasa koyucuların izleyebileceğinden çok daha hızlı şekillendirdiği günümüzde özellikle dikkat çekicidir. Bazen kurallar yürürlüğe girmeden önce bile eski hale gelir. İnternet düzenlemesinde yasal eskime riski önemli bir husustur.

Sosyal normlar (gelenekler)

Mevzuat gibi, sosyal normlar da belli davranışları yasaklamaktadır. Mevzuattan farklı olarak, hiçbir devlet gücü bu normları uygulamaz. Eşitler arasında baskı yoluyla toplum tarafından uygulanmaya zorlanırlar. İnternetin ilk günlerinde, internet etiği olarak etiketlenen internetin kullanımına ilişkin “akran baskısı” ve “dışlama”nın temel yaptırımlar olduğu bir dizi sosyal norm ortaya çıkmıştır. İnternet’in öncelikle nispeten küçük, çoğunlukla akademik topluluklar tarafından kullanıldığı bu dönemde, sosyal normlar yaygın olarak gözlenmiştir. İnternetin büyümesi bu kuralları etkisiz hale getirmiştir. Bununla birlikte, bu tür bir düzenleme, güçlü topluluk bağlarına sahip sınırlı gruplar içinde kullanılabilir. Örneğin, Wikipedia topluluğu, Wikipedia makalelerinin nasıl düzenlendiğini ve makaleler üzerinde çatışmaların nasıl çözümlendiğini düzenleyen sosyal normlar tarafından yönetilir. Politika ve kılavuzları kodlayarak, Wikipedia normları giderek kendi kendini düzenlemeye dönüşmüştür.

Öz düzenleme

ABD hükümetinin ICANN’ın kuruluşuna zemin hazırlayan 1998 *İnternet Yönetişimi Beyaz Kitabı*,⁵ İnternet için tercih edilen düzenleyici mekanizma olarak öz düzenlemeyi getirmiştir.

Öz düzenlemenin sosyal normlar ile ortak unsurları vardır. Temel fark, tipik olarak yapışkan ve dağınık kuralları içeren sosyal normların aksine, öz düzenlemenin açık ve iyi düzenlenmiş bir kurallar kümesine dayanmasıdır. Kendi kendini düzenleme genellikle uygun etik davranış biçimi olarak kabul edilen kuralları belirler.

Kendi kendini düzenleme eğilimi, ISS'ler arasında özellikle belirgindir. Pek çok ülkede, ISS'ler, içerik politikası ile ilgili kuralları uygulamak için devlet yetkilileri tarafından baskı altındadır. ISS'ler bu baskıya kendi düzenlemeleri yoluyla, müşterileri için belirli davranış standartları uygulayarak cevap vermeye çalışmaktadır.

Öz düzenleme faydalı bir düzenleme tekniği olsa da, içerik politikası, ifade özgürlüğü ve mahremiyetin korunması gibi yüksek kamu yararı olan alanları bu yolla düzenlemek bazı riskler içermektedir. Öz düzenlemeye güvenmek, aşağıdaki gibi birkaç soruyu gündeme getirir: ISS'ler yasal makamlar yerine kararlar alabilir mi ve karar vermeli mi? Kabul edilebilir içeriğin ne olduğunu yargılayabilir mi ve yargılamalı mı?

İçtihatlar

İçtihatlar (mahkeme kararları), İnternet ile ilgili yasal gelişmeler üzerinde önemli bir etkiye sahiptir. Erken evrelerde, İnternet gelişmelerinin çoğunun ABD'de gerçekleştiği zamanlarda, ABD hukuk sisteminin temel taşı olan içtihat, İnternetle ilgili yasal gelişmelerde kilit rol oynamıştır. İnternet, yeni bir fenomen olarak mahkeme davalarıyla (Anglo-Saxon yasasında emsaller) düzenlenmiştir. Hakimler, gerekli araçlara, yani yasal kurallara sahip olmasalar bile davalara karar vermek zorunda kaldılar. Emsalleri aracılığıyla, yeni yasal düzenlemeler geliştirmeye başlamışlardır.

Daha yakın zamanlarda, Avrupa mahkemelerinin içtihatları çevrimiçi yasal gelişmeler için özellikle önem kazanmıştır. Örneğin, Mayıs 2014 tarihli bir CJEU kararı, Avrupa'daki ve diğer ülkelerdeki çevrimiçi içeriğe ilişkin sonuçlarla unutulma hakkı ya da daha kesin olarak endeksten çıkarılma hakkı konusunda yeni kuralları getirmiştir. ABD ile AB arasındaki Güvenli Liman anlaşmasını geçersiz kılan Ekim 2015'teki bir başka karar da, iki tarafın Atlantik'te kişisel verilerin aktarılması konusunda yeni bir anlaşma üzerinde müzakere etmeye ve uzlaşmaya zorlamasına benzer bir etkiye sahiptir.

Mahremiyet ve veri koruması konusundaki CJEU Kararları ile ilgili daha fazla tartışma için 8. Bölüme bakınız.

Uluslararası yasal enstrümanlar

İnternet faaliyetlerinin sınır ötesi niteliği, uluslararası yasal araçların kullanılması gereğini işaret etmektedir. Uluslararası hukuk tartışmalarında, önemli sonuçlara yol açabilecek terminolojik bir karışıklık vardır. Uluslararası hukuk terimi, genellikle antlaşmalar ve sözleşmelerin kabulü ile ulus devletler tarafından kurulan uluslararası kamu hukuku ile eşanlamlı olarak kullanılmaktadır. Uluslararası kamu hukuku, İnternet'in telekomünikasyon, insan hakları ve siber suçlar da

dahil olmak üzere birçok alanına uygulanmaktadır. Bununla birlikte, uluslararası özel hukuk, İnternet meseleleriyle ilgilenmek için daha fazla olmasa da, aynı derecede önemlidir, çünkü İnternete ilişkin çoğu mahkeme davası sözleşmeler, haksız fiil ve ticari sorumluluklar gibi hususları içermektedir.

Uluslararası özel hukuk

İnternetin küresel doğası göz önüne alındığında, farklı ulusal yargı alanlarından bireyleri ve kurumları içeren yasal anlaşmazlıklara sıkça rastlanmaktadır. Uluslararası özel hukuk kuralları, (farklı ülkelerden iki veya daha fazla varlığı içeren yasal ilişkiler gibi) yabancı unsurlarla ilgili yasal davalarda, örneğin (Facebook, Twitter gibi kullanıcıları tüm dünyaya yayılmış) internet şirketleri arasındaki davalarda yargıyı kimin vereceği gibi, uygulanabilir yargı ve hukuk oluşturmak için kriterleri belirlemektedir. Yargı yetkisi kriterleri, (milliyet, ikametgah gibi) bireysel ve ulusal yargı arasındaki bağlantıyı ve (sözleşmenin yapıldığı yer, mal alışverişinin yapıldığı yer gibi) belirli bir işlem veya ulusal yargı arasındaki bağlantıyı içermektedir.

Bununla birlikte, İnternet tabanlı sorunları çözmek için uluslararası özel hukuk nadiren yalnızca kullanılmıştır, çünkü prosedürleri genellikle karmaşık, yavaş ve pahalıdır. Uluslararası özel hukukun ana mekanizmaları, sınır ötesi etkileşimin sık ve yoğun olmadığı bir zamanda geliştirildi ve orantılı olarak daha az sayıda vaka farklı yargı alanlarından bireyleri ve varlıkları içermektedir. İnternete ilişkin yasal davalarda hukuki düzeltmenin sağlanması için uluslararası özel hukukun daha hızlı, daha ucuz ve daha esnek olması gerekmektedir.

Uluslararası kamu hukuku

Uluslararası kamu hukuku ulus devletler arasındaki ilişkileri düzenlemektedir. Bazı uluslararası kamu hukuku enstrümanları halihazırda (telekomünikasyon düzenlemeleri, insan hakları sözleşmeleri, uluslararası ticaret anlaşmaları gibi) İnternet yönetişimi ile ilgili alanlarla ilgilenmektedir. İnternet yönetişimi için antlaşmalar ve sözleşmeler, geleneksel yasalar, yumuşak yasalar ve (zorlayıcı yasa - kalıcı bir norm demek olan) ius cogens dahil olmak üzere bir dizi uluslararası kamu hukuku kullanılabilir.

Uluslararası konvansiyonlar (uygulamalar)

Uluslararası sözleşmeler yasal olarak devletler arasında bağlayıcı anlaşmalardır. Bazıları tarafından İnternet ile ilgili konularla ilgili olarak görülen ana sözleşmeler, ITU'nun ITR'leridir. 1988'de, İnternet hala gelişimin ilk aşamalarında iken, ITR'ler İnternet üzerinde belirli hükümler içermiyordu. İnternetin WCIT-12'de açık bir şekilde yer alması için ITR'lerin genişletilmesi gerektiğine dair tartışmalar yapılmıştır. O zaman, İnternetin nasıl işlediği, temel prensipleri ve ayrıca İnternet güvenliği ve İnternet içeriği ile ilgili konular üzerinde önemli bir etkisi olabilecek birçok teklif yapılmıştır. Üye devletler bu konuda bir anlaşmaya varamamış ve revize edilmiş 2012 ITR'leri yine de internete açık referanslar içermemiştir. Bununla birlikte, bazı ITU üyeleri, gözden geçirilmiş ITR'lerde yer alan birkaç hükümün, kendi görüşlerine göre ITU faaliyetleri kapsamı dışında olması gereken İnternet ile ilgili hassas konuları kapsayan bir

potansiyel olarak yorumlanabileceğini belirtmiştir.⁶ Bu devletler revize edilmiş yönetmelikleri imzalamamaya karar vermiş, böylece 1988 versiyonuna bağlı kalmaya devam etmiştir.

ITU sözleşmelerinin yanı sıra, doğrudan İnternet ile ilgili konularla ilgilenen tek sözleşme, CoE [Siber Suçlar Konvansiyonu Sözleşmesi](#)'dir. Bununla birlikte, birçok başka uluslararası yasal araç, İnternet Şartları için, BM Şartı'ndan, örneğin insan hakları, ticaret ve IPR ile ilgili daha spesifik araçlara kadar geçerlidir.

Uluslararası teamül hukuku

Geleneksel hukukun gelişimi iki unsur içerir: genel uygulama (consuetudo) ve bu uygulamanın yasal olarak bağlayıcı olduğunu kabul etme (opinio juris). Geleneksel hukukun ortaya çıkması için genellikle uzun bir süre gerekir. Örneğin, Deniz Yasası kuralları, yüzyıllar boyunca, ulusal yönetimler tarafından kurulan uygulamalar yoluyla, bu kurallar Birleşmiş Milletler Deniz Yasası Kanunu'nda (1982) kodlanıncaya kadar kristalize edildi. Bununla birlikte, modern gelişmelerin daha hızlı olması, geleneksel kuralların geliştirilmesi için daha kısa bir zaman aralığı gerektirmektedir. Hızlı İnternet büyümesi ile gümrük hukukunun yavaş gelişme süreci arasındaki gerilimin üstesinden gelmek için olası bir çözüm, diritto spontaneo ya da 'anlık geleneksel uluslararası hukuk' kavramını tanıtan İtalyan hukukçi Roberto Ago tarafından önerilmiştir.⁷

Bağlayıcı olmayan hukuk

İnternet yönetişimi tartışmalarında "yumuşak hukuk" terimi sıklıkla kullanılmaktadır. Yumuşak hukukun çoğu tanımı ne olmadığı üzerine odaklanır: yasal olarak bağlayıcı bir araç değildir. Tipik olarak, yumuşak hukuk enstrümanları genellikle beyanlar ve kararlar gibi uluslararası belgelerde bulunan prensipleri ve normları içerir. Yasal olarak bağlayıcı olmadığı için, uluslararası hukuk veya diğer uyumsuzluk çözüm mekanizmalarıyla yumuşak yasalar uygulanamaz.

Nihai Deklarasyon, Cenevre Eylem Planı, Bilgi Toplumu için Tunus Gündemi ve Bölgesel Deklarasyonlar da dahil olmak üzere ana WSIS belgeleri, belirli yumuşak yasa normları geliştirme potansiyeline sahiptir. Yasal olarak bağlayıcı değildirler, ancak bunlar genellikle uzun süren müzakerelerin ve ulus devletlerin kabul etmesinin sonucudur. Ulus devletlerin ve diğer paydaşların yumuşak hukuk araçlarını müzakere etmek ve gerekli bir uzlaşmaya varmak zorunda olmaları taahhüdü, bu tür belgelerin basit siyasi beyanlardan daha fazla olduğu düşüncesinin ilk unsurunu oluşturmaktadır.

Yazılım hukuku, İnternet yönetişimi konularının ele alınmasında bazı avantajlar sağlamaktadır. Birincisi, devletler tarafından onaylanmayan ve dolayısıyla uzun süreli müzakereler gerektirmeyen daha az resmi bir yaklaşımdır. İkincisi, yeni yaklaşımların test edilmesini kolaylaştıracak ve İnternet yönetişimi alanındaki hızlı gelişmelere uyum sağlayacak kadar esnektir. Üçüncüsü, yumuşak yasalar, çok paydaşlı bir yaklaşım için devletler ve uluslararası örgütlerle sınırlı uluslararası yasal bir yaklaşımdan daha fazla fırsat sağlar.

Üstün hukuk

Üstün hukuk, *Viyana Antlaşmalar Hukuku Sözleşmesi*'nin⁸ 53. Maddesindeki “dokunulmasına izin verilmeyecek ve sadece aynı özellikteki genel uluslararası hukuk normlarıyla değiştirilebilecek Devletler topluluğu tarafından kabul edilmiş ve tanınmış bir norm” olarak tanımlanmıştır. Oxford Üniversitesi'ndeki All Souls College eski üyesi Profesör Ian Brownlie, üstün hukuk urallarına ilişkin aşağıdaki örnekleri sıralamıştır:

- Güç kullanımının yasaklanması.
- Soykırım yasası.
- Irk ayrımının yapılmaması ilkesi.
- İnsanlığa karşı işlenen suçlar.
- Korsanlığı ve köle ticaretini yasaklayan kurallar⁹

İnternet yönetiminde üstün hukuk, onun tarafından yasaklanan faaliyetlerin (soykırım, ırk ayrımcılığı, kölelik vb.) organizasyonunu teşvik eden ve/veya kolaylaştıran çevrimiçi faaliyetlerle başa çıkma ile ilgili olabilir.

Yargı

Yargı yetkisi mahkeme ve devlet organlarının yasal davalara karar verme yetkisidir. Yargı ile İnternet arasındaki ilişki, yargı alanı baskın olarak ulusal coğrafyaları ilgilendirdiğinden belirsiz kalmıştır.

Her devlet kendi ülkesinde yargı yetkisini kullanma hakkına sahiptir. Bununla birlikte, İnternet, kayda değer miktarda sınır aşan değiş tokuşu kolaylaştırdığı için geleneksel hükümet mekanizmaları aracılığıyla izlenmesi (imkansız olmasa da) zor bir araçtır. İnternet konusunda yargılama sorunu, İnternet yönetişimi ile ilgili merkezi ikilemlerden birini vurgulamaktadır: İnterneti mevcut yasal ve politik coğrafyaya bağlamak nasıl mümkün olabilir?¹⁰

Son yıllarda, mahkemeler güçlü bir yargı unsuru ile gittikçe artan sayıda dava ile karşı karşıya kalmaktadır. Unutulma hakkı konusundaki kararlar, diğer yargı bölgelerinde yer alan verileri talep eden makamları içeren davalar ve Güvenli Liman Çerçevesinin geçersiz kılınması dikkate değer örneklerdir. Bu gibi durumlarda, yargının “kolu” ulusal coğrafyanın veya AB topraklarının ötesine uzamıştır.

Bu davaların birçoğu, Avrupa mahkemelerinde sayısız sonuçlara yol açmıştır:

- Avrupa mahkemeleri, ABD şirketlerini içeren gittikçe artan sayıda dava üzerinde yargı yetkileri olduğunu ileri sürmektedir.
- Avrupa'da düzenleyicilerin, özellikle veri koruma yetkililerinin rolü daha belirgin hale gelmiştir.
- İnternet ile ilgili konularla küresel hukuk giderek Avrupa mahkemeleri tarafından şekillenmektedir.

Yargı ilkeleri

Yargı yetkisine karar verirken üç ana husus önemlidir:

- Hangi mahkeme veya devlet gerçek yetkilidir? (prosedürel yargı)
- Hangi kurallar uygulanmalıdır? (esasa ilişkin yargı)
- Hangi mahkeme kararları uygulanmalıdır? (yaptırıma ilişkin yargı)
-

Belirli durumlarda, aşağıdaki kriterler yargı tesis eder:

- **Bölgesel Prensip** - devletin kendi bölgesindeki insanları ve mülkleri yönetme hakkı.
- **Şahsilik İlkesi** - Devletin, vatandaşları üzerinde olabilecekleri yerde karar verme hakkı (milliyet ilkesi).
- **Etkiler İlkesi** - Devletin, yurtdışında yürütülen faaliyetlerden kaynaklan, kendi topraklarında ekonomik ve yasal etkilere neden olan meseleri yönetme hakkı.

Modern uluslararası hukukun getirdiği bir diğer önemli ilke, **evrensel yargı yetkisidir**¹¹. ‘Evrensel yargı yetkisi kavramı, geniş anlamda, herhangi bir yerde ve her kim tarafından olursa olsun, herhangi bir şekilde, bölge, milliyet veya özel devlet çıkarlarıyla herhangi bir bağlantıya ihtiyaç duyulmadan işlenen suçları cezalandırma yetkisidir.’¹²

Evrensel yargı, korsanlık, savaş suçları ve soykırım gibi suçları kapsar. Bununla birlikte, İnternet fonksiyonel olarak erişilebilirlik ilkesine dayanan çok daha geniş bir dava kümesine evrensel yargı yetkisi getirmiştir. Bu ilkeye göre, İnternet’e belirli bir ülkeden erişmek, ülke mahkemelerinin yargı yetkisi için yeterli temeldir. Bu ilke, eData ve Pinckney¹³ ve CJEU¹⁴ davaları kadar Yahoo! davasına¹⁵ da bir Fransız mahkemesi tarafından uygulanmıştır. İnternet erişimi gibi sınırlı bir ölçütle yargı yetkisine başvurma olasılığı, forum alışverişi de dahil olmak üzere çeşitli sorunlara yol açabilir. Yani, dava, İnternet erişimi olan herhangi bir ülkeden başlatılabilir.

Yargı uyumsuzluğu

Yargı uyumsuzluğu, birden fazla devlet belirli bir davada yargı yetkisi talep ettiğinde ortaya çıkar. Bu genellikle yasal bir durum için (farklı devletlerden bireyleri veya uluslararası işlemler içermesi gibi) fazladan bir bölgesel bileşen içerdiğinde gerçekleşir. İlgili yargı, şu unsurlardan biri tarafından belirlenir: bölge, milliyet veya bir eylemin etkisi. İçeriği yerleştirirken veya İnternet’le etkileşime girerken, varsa hangi ulusal kanunun ihlal edilebileceğini bilmek zordur. Bu bağlamda, hemen hemen her İnternet etkinliğinin, çoklu yargılama yetkisi veya sözde dağılma etkisi yaratacak uluslararası bir yönü vardır.¹⁶

Yargı ve içeriğe ulaşma

Birden fazla yargı alanı sorununu örnekleyen erken ve sıkça alıntı yapılan davalardan biri Fransa’da 2001’deki Yahoo! davasıdır. Nazi objelerinin sergilenmesini ve satılmasını yasaklayan Fran-

sız yasalarının ihlali söz konusuydu, bu tür materyali sağlayan Yahoo.com açık artırma sitesi bu tür malzemelerin gösterilmesinin yasal olduğu ABD’de bulunuyordu. Dava (coğrafi konum yazılımı ve erişimin filtrelenmesi gibi) teknik bir yöntem kullanılarak çözüldü. Yahoo! Fransa’dan siteye erişen kullanıcıları tespit etmek ve Nazi materyallerini gösteren web sayfalarına erişimlerini engellemek zorunda kaldı.¹⁷

Benzer şekilde, unutulma yargısı (Google ve ortaklarının, Mario Costeja Gonzalez ve ortaklarına karşı davası), arama motorlarına Avrupalı kullanıcılardan aramalardan belirli sonuçları çıkarma isteklerini değerlendirme zorunluluğu getirmiştir. Karar, Avrupa’daki veri koruma makamlarının kararları ile daha da şekillenmiştir. Yahoo! ‘da kullanılabenzer bir akıl yürütme ile Fransız yargısı sonuçların çıkarılmasının yalnızca (.fr, .es ve .uk gibi) Avrupa uzantıları için değil dünya genelinde Google tarafından uygulanmasına hükmetmiştir.¹⁸

Yargı ve veri koruma

AB vatandaşlarının Avrupa sınırlarının ötesinde depolanan kişisel verilerinin korunması, son yıllarda en çok tartışılan davaların bazılarında katkıda bulunmuştur. 2013’te bir Avusturya vatandaşı olan Maximilian Schrems, İrlanda Veri Koruma Komiseri’nden Facebook’un kişisel verilerini ABD’ye aktarmasını yasaklamasını isteyen bir şikayette bulundu. Schrems, ABD’nin, kullanıcıların ABD yasalarına göre kitlesel denetime tabi tutulması nedeniyle, kullanıcıların verileri için yeterli koruma sağlamadığını savundu. Komisyon Üyesi talebi reddettiğinde, Schrems kararı mahkemeye taşıdı. Dava sonunda, AB ile ABD arasında kişisel verilerin transferini yöneten Güvenli Liman Çerçevesi’nin geçersiz olduğuna karar veren CJEU’ya getirildi.¹⁹ Bu, Güvenli Liman anlaşmasının daha sonra AB ABD Mahremiyet Kalkanı Çerçevesi ile değiştirilmesine neden oldu.

Veri korumaya ilişkin düşünceler iki gelişmeye katkıda bulunmuştur. Birincisi, birkaç şirketin veri merkezlerini ve veri işleme işlevlerini, özellikle de İrlanda olmak üzere daha rahat bir düzenleyici yaklaşım benimseyen bölgelere taşımış olmalarıdır. Bu, şirketleri mahkeme davalarından korumadıysa da, Microsoft’u içeren 2016’daki dava kararı ABD’nin İrlanda’da depolanan verilere erişim sağlamak için yerel bir arama emri kullanamayacağını teyit etmiştir.²⁰

İkincisi, Çin ve Rusya gibi bazı ülkelerin, kullanıcıların verilerinin yerel olarak depolanmasını gerektiren yasaları çıkarmasıdır. Ulusal topraklarda bulunan sunuculardaki verilerin depolanması, Çin’in siber egemenliğin sağlanmasına yönelik politikasının önemli bir dayanağıdır.

Yargı ve kullanım koşulları

Şirketlerin kullanım koşullarındaki yargı yetkisi, Facebook’u da kapsayan birçok mahkeme davasında mahkeme kararlarında yer almıştır.

Öne çıkan bir olay, Musée d’Orsay müzesinde asılı olan çıplak resim imajlarını yayınladıktan sonra Facebook hesabı askıya alınan bir Fransız öğretmenin davasıydı. Paris Temyiz Mahkemesi, Facebook’un Fransa’da dava edilebileceğine hükmetmiş ve sosyal ağın kullanım şartlarının

yargı yetkisinin Kaliforniya'da bulunduğu iddiasını reddetmiştir.²¹ Fransa mahkemesi, ABD mahkemesi dışındaki şirket aleyhindeki diğer davaların önünü açmıştır.

2016 yılının Haziran ayında, bir İsrail mahkemesi, Facebook'un Kaliforniya mahkemelerinde dava açılmasına ilişkin kullanım şartlarındaki hükümlerinin bir fıkrasının geçersiz olduğuna ve Facebook aleyhine toplu dava açılmasına karar vermiştir.²² Dava, Facebook'un önceden izin almaksızın kullanıcıların hangi reklamları görmesi gerektiğini belirlemek için özel ilanları kullanarak kullanıcıların gizliliğini ihlal ettiğini iddia etmiştir.

Coğrafi konum ve filtreleme teknikleri gibi teknik çözümlerin yanı sıra, yargı ihtilafının çözümüne yönelik diğer yaklaşımlar, ulusal yasaların uyumlaştırılmasını ve alternatif uyuşmazlık çözüm mekanizmalarının kullanımını içermektedir.

Ulusal yasaların uyumlaştırılması

Ulusal yasaların uyumlaştırılması küresel düzeyde bir uyumlu kurallar dizisinin oluşturulmasına neden olabilir. Uyumlaştırılmış kurallar uygulandığında, yetki alanı sorunu daha az önemli olacaktır. Örneğin, çocuk cinsel istismarı içeriği, korsanlık, kölelik ve terörizm gibi yüksek düzeyde küresel fikir birliğinin var olduğu alanlarda uyum sağlanabilir. Görüşler, siber suç gibi diğer konularda da yaklaşmaktadır. Bununla birlikte, içerik politikası dahil olmak üzere bazı alanlarda, kültürel farklılıkların çevrimiçi ortamda çevrimdışı dünyadan daha belirgin biçimde çarpışmaya devam etmesi nedeniyle, temel kurallar konusunda küresel bir uzlaşmaya varılması pek olası değildir.²³

Uyum eksikliğinin diğer bir olası sonucu, içeriğin daha düşük İnternet düzenlemesi seviyesine sahip ülkelere taşınmasıdır. Deniz Kanunu analojisini kullanırsak, bazı ülkelerin çevrimiçi içerik için "kolaylık sağlayan bayrakları" olabilir.

www.igbook.info/jurisdiction

Alternatif uyuşmazlık çözümleri

Alternatif uyuşmazlıkların çözümü (ADR) geleneksel mahkemelerin yerine kullanılabilen bir mekanizmadır. ADR araçları tahkim ve aracılık içerir. Çevrimiçi uyuşmazlık çözümü (ODR), uyuşmazlıkların çözümünde İnternet ve teknolojiyi kullanır.

İnternet davaları söz konusu olduğunda, bu mekanizmalar - özellikle tahkim - mevcut uluslararası özel hukukun sayısız İnternet davalarıyla ilgilenememesi nedeniyle ortaya çıkan boşluğu doldurmak için yoğun olarak kullanılmaktadır. Bir örnek, alan adı kayıtları ile ilgili konularda WIPO ve ICANN tarafından birincil uyuşmazlık çözümü prosedürü olarak geliştirilen UDRP'dir.

Tahkimde kararlar, taraflarca seçilen bir veya daha fazla bağımsız birey tarafından verilir. Mekanizma genellikle tahkim yeri, prosedürler ve hukuk seçimi gibi hususları da belirten özel bir sözleşmede belirlenir. Ticari sektördeki uluslararası tahkim uzun zamandır devam eden bir geleneğe sahiptir.

Tablo 2, geleneksel mahkeme sistemleri ve tahkim arasındaki temel farklılıklara kısa bir genel bakış sunmaktadır.

Tablo 2. Mahkeme ve tahkim arasındaki farklar

Unsur	Mahkeme	Tahkim
Organizasyon	Ulusal kanun ve anlaşmalar ile kurulmuştur	Kalıcı ve ad hoc tahkim (kurulmuş ve/veya taraflarca seçilmiş)
Geçerli yasa	Mahkeme hukuku (hakim yürürlükteki kanuna göre karar verir)	Taraflar hukuk yolunu seçebilir; eğer seçmezlerse, sözleşmede belirtilen kurallar geçerlidir; bir niyet yoksa, tahkim yasası geçerlidir
Prosedür	Yasa/anlaşmalarla oluşmuş mahkeme prosedürleri	Taraflarca kararlaştırılır (geçici, ad hoc biçimde) Tahkim organı düzenlemesi ile (kalıcı biçimde) kararlaştırılır
Uygulama	Ulusal otoriteler tarafından uygulanır	Tahkim anlaşması ve New York Sözleşmesi uyarınca uygulanır

Geleneksel mahkemelere kıyasla tahkim, daha fazla esneklik, daha düşük harcama, hız, yargı seçimi ve yabancı tahkim kararlarının daha kolay uygulanmasını içeren birçok avantaj sunmaktadır.

Tahkimin temel avantajlarından biri, potansiyel yargı ihtilafının üstesinden gelmesidir. Tahkim, İnternet ile ilgili mahkeme davalarında en zor görevlerden biriyle - mahkeme kararlarının uygulanmasıyla ilgili belirli avantajlara sahiptir. [Yabancı Tahkim Kararlarının Tanınması ve Uygulanmasına İlişkin New York Sözleşmesi](#),²⁴ tahkim kararlarının uygulanmasını düzenlemektedir. Bu sözleşmeye göre, ulusal mahkemeler tahkim kararlarını uygulamakla yükümlüdür. Yabancı ülkelerde mahkeme kararını uygulamak yerine, New York Sözleşmesi rejimini kullanarak yabancı ülkelerde tahkim kararlarını uygulamak genellikle daha kolaydır.

Tahkimin temel sınırlılığı, insan haklarının korunması gibi kamu yararı yüksek konulara değinmemesidir; bunlar devlet tarafından kurulmuş mahkemelerin müdahalesini gerektirir. Başka sınırlılıklar da şunlardır:

- Tahkim genellikle ön anlaşmayla kurulduğu için, taraflar arasında önceden herhangi bir anlaşmaya yoksa (hakaret, çeşitli sorumluluk türleri, siber suç gibi) geniş bir sorun alanını kapsamaz.
- Birçok kişi, mevcut tahkim şartını normal sözleşmelere ekleme uygulamasının (genellikle bir İnternet kullanıcısı veya bir e-ticaret müşterisi gibi) sözleşmedeki zayıf taraf için dezavantajlı olarak değerlendirmektedir.

- Bazıları tahkimin (ABD/İngiltere yasal sistemi gibi) içtihad temelli hukukun ötesine geçtiği ve diğer ulusal yasal sistemleri kademeli olarak bastırdığı endişesini duymaktadır. E-ticaret durumunda, bu, daha önce geçerli olan kanunlarda ticari düzenlemelerin zaten yüksek düzeyde uyumlaştırılması göz önüne alındığında, daha kabul edilebilir olabilir. Bununla birlikte, içtihad hukukunun genişlemesi ulusal hukuk sisteminin belirli bir kültürel bağlamı yansıttığı İnternet sözleşmesi gibi sosyo-kültürel konularda daha hassas hale gelmektedir.

Tahkim, ticari ihtilaflarda yaygın olarak kullanılmaktadır. Ticari anlaşmazlıklar ile ilgilenen gelişmiş bir kurallar ve kurumlar sistemi vardır. Başlıca uluslararası araç, Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu'nun (UNCITRAL) 1985'de çıkardığı [Uluslararası Ticari Tahkim Yasasıdır](#).²⁵ Önde gelen uluslararası tahkim, genellikle ticaret odalarına bağlıdır.

ADR, ODR, ve İnternet

Tahkim ve diğer alternatif uyuşmazlık çözüm sistemleri İnternet ile ilgili davalarda yaygın olarak kullanılmaktadır ve daha önce belirtilen UDRP bu konuda bir örnektir. Aralık 1999'da UDRP kapsamında çalışmaların başlamasından bu yana, WIPO Tahkim ve Arabuluculuk Merkezi, 35.000'den fazla alan adı davasını çözmüştür.²⁶

UDRP, alan adlarının gTLD'ler (ör. .Com, .edu, .org, .net) ve bazı ccTLD'ler altında tescili ile ilgili tüm sözleşmelerde bir uyuşmazlık çözüm mekanizması olarak öngörülmektedir. Bunun benzersiz yönü, tahkim kararlarının, (etki alanı adının iptali veya etki alanı adı tescilinin şikayetçiye devredilmesi gibi) ulusal mahkemelere gidilmeden ihtilaflı etki alanı adıyla ilgili değişikliklerle doğrudan çözüm getirmesidir.

AB, 2016 yılında yeni bir uyuşmazlık çözümü platformunu devreye sokmuştur. Şubat 2016'dan bu yana faaliyet gösteren Çevrimiçi Uyuşmazlık Çözümü platformu, tüketicilerin ve tüccarların çevrimiçi yurt içi ve sınır ötesi alımlar konusundaki çevrimiçi uyuşmazlıklarını çözmelerine yardımcı olmayı amaçlamaktadır.²⁷

Bazı İnternet şirketleri (örneğin Google, Facebook ve Twitter) da kendi mekanizmalarını geliştirmiştir. CJEU'nun unutulmaya karar vermesinin ardından Google, bireylerin web sitelerinin arama sonuçlarından kaldırılmasını talep etmelerini sağlayan özel bir mekanizma kurdu. Mayıs 2014 - Ekim 2016 arasında Google, kaldırılması için 575.000'den fazla talep almıştır.²⁸

Bu uyuşmazlık çözümü uygulaması çok çeşitli sorular açmıştır: Özel şirketler uyuşmazlık çözümü sağlamalı mıdır? Uygulanacak usule ilişkin ve esas kurallar nelerdir? Etkilenen İnternet kullanıcıları için bu mekanizmalara erişim nasıl sağlanabilir?

www.igbook.info/arbitration

Fikri mülkiyet hakları

Bilgi ve fikirler, küresel ekonomideki kilit kaynaklardır. Bilgi yönetimi ve fikirlerin ifade edilmesinin, IPR yoluyla korunması, İnternet yönetişimi tartışmalarında baskın konulardan biri haline gelmiştir ve güçlü, kalkınma odaklı bir bileşene sahiptir. IPR, İnternet'in gelişiminden,

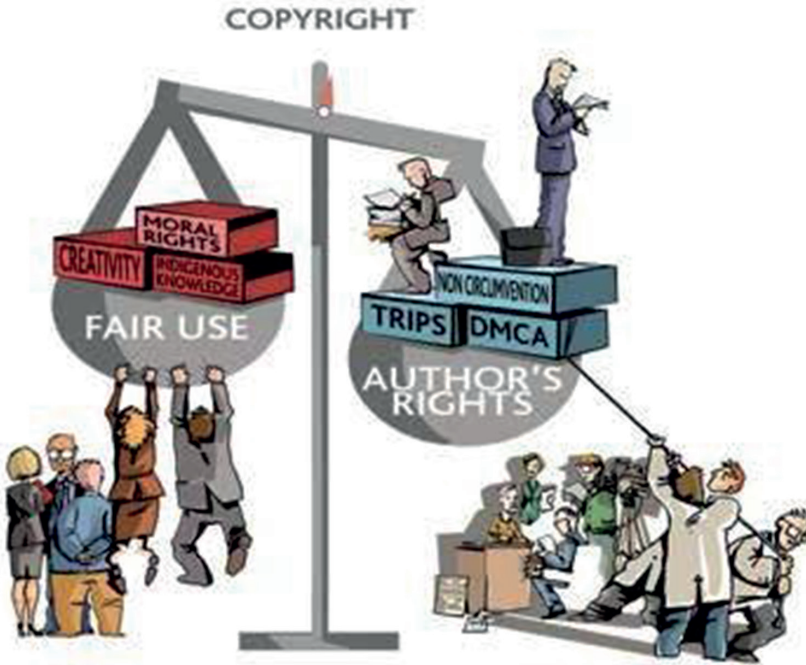
özellikle bilgi ve bilgilerin dijitalleştirilmesinden ve ayrıca manipülasyonları için yeni olasılıklardan etkilenmiştir. İnternet ile ilgili IPR, telif hakkı, ticari markalar ve patentler içerir. Diğer IPR tasarımları, faydalı modelleri, ticari sırları, coğrafi endikasyonları ve bitki çeşitlerini içerir.

Telif hakkı

Telif hakkı, yaratıcıların orijinal eserleri üzerindeki haklarını tanımlayan yasal bir terimdir. Telif hakkı, bir fikrin ifadesini yalnızca kitap, CD veya bilgisayar dosyası gibi çeşitli biçimlerde gerçekleştirildiği zaman korur. Fikrin kendisi telif hakkıyla korunmaz. Bununla birlikte, pratikte, fikir ile fikrin ifadesi arasında açık bir ayrım yapmak bazen zordur.

Telif hakkı rejimi, teknolojinin gelişimini yakından takip etmiştir. Matbaa, radyo, televizyon ve VCR gibi her yeni buluş, telif hakkı kurallarının hem biçimini hem de uygulamasını etkilemiştir. İnternet istisna değildir. Geleneksel telif hakkı kavramı, web'den metinlerin kesilmesi ve yapılandırılması kadar basit olanlardan, müzik ve video materyallerinin İnternet üzerinden yoğun bir şekilde dağıtılması gibi daha karmaşık etkinliklere kadar pek çok yolla sorgulanmaktadır.

İnternet ayrıca, telif hakkı sahiplerine, telif hakkı olan materyallerin kullanımını korumak ve izlemek için daha güçlü teknik araçlar sağlayarak güç vermektedir. Bu gelişmeler, telif hakkı yasasının temeli olan yazarların hakları ile kamu yararı arasındaki hassas dengeyi tehlikeye atmaktadır (Şekil 17).



Şekil 17. Telif hakkı

Bugüne kadar, büyük rekor ve multimedya şirketleri tarafından temsil edilen telif hakkı sahipleri, IPR'lerini korumada çok aktif olmuştur. Kamunun çıkarları genellikle belli belirsiz algılandı-ğı ve yeterince korunmadığı şeklinde görülmektedir. Bununla birlikte, bu, temel olarak, bilgiye ve bilgiye açık erişime odaklanan çok sayıda küresel girişimle (örneğin, Creative Commons) bu algı değişmektedir.

Mevcut durum

Ulusal ve uluslararası düzeyde daha katı telif hakkı koruması

Kayıt ve eğlence endüstrileri, telif hakkı korumasını güçlendirmek için ulusal ve uluslararası düzeyde yoğun şekilde lobi faaliyetleri yürütmektedir. Uluslararası düzeyde, dijital eserlerin korunması [WIPO Telif Hakkı Antlaşması](#)'nda²⁹ (1996) gündeme getirilmiştir. Bu anlaşma ayrıca, yazarların münhasır haklarının sınırlılıkları için daha katı hükümler, telif hakkının teknolojik korumasını aşmanın yasaklanması ve diğer ilgili önlemler gibi telif hakkı koruma rejiminin sıkılaştırılması için hükümler içermektedir. Bölgesel düzeyde, Şubat 2016'da imzalanan 12 Pasifik Kıyı ülkesi arasındaki bir ticaret anlaşması olan [Trans-Pasifik Ortaklığı Anlaşması](#)'ndaki IPR hükümleri, telif hakkı süresini artırmak için ek olarak zorlayıcı kuralları barındırmaktadır.³⁰ ABD'de, 1998'in ABD [DMCA](#)'sı³¹ ile telif hakkının daha sıkı korunması sağlanmıştır.

İnternet araçlarını telif hakkıyla korunan içeriğin yayılmasını filtrelemeye veya izlemeye zorlayarak daha sıkı bir kontrol uygulanmasını amaçlayan ulusal ve uluslararası düzeyde çeşitli düzenlemeler önerilmiştir. Bu öneriler yönetmeliklerin kabul edilmesini durduran güçlü halk protestosunu tetiklemiştir. 2011'de ABD'de web sitelerine girişin engellenmesi ve arama motorlarının bu sitelere bağlanmasını yasaklanması da dahil internet sitelerinde korsanlıkla mücadele etmenin yeni yollarını bulan iki sözleşme desteklenmiştir: [SOPA](#)³² ve [PROTECT IP Yasası](#) (PIPA).³³ Her iki sözleşme de protestoların ardından ertelenmiştir. Uluslararası düzeyde, ACTA, IPR ihlallerini özel (şirketler) icra ve polislik faaliyetlerine imkan tanıyacak şekilde ele almaya çalışmıştır. Avrupa'daki güçlü protestoların ardından Avrupa Parlamentosu [ACTA](#)'ya³⁴ karşı oy kullanmıştır.

Bu düzenleyici eylemler, akademisyenler ve sivil özgürlük grupları tarafından insan hakları ve özgürlükler temelinde sert bir şekilde eleştirilmiştir. Bireysel İnternet kullanıcıları çevrimiçi ve çevrimdışı protestolara katılmıştır.³⁵

Telif hakkı ihlallerine karşı yazılım

Telif hakkı failleri, örneğin müzik ve videoları yasa dışı olarak çevrimiçi dağıtmak için yazılım araçları kullanır. Telif hakkı savunucuları da yazılımı kullanabilir. Geleneksel olarak, devlet yetkilileri ve işletmeler bu alandaki sorumluluklarını yasal mekanizmalarla yerine getirmişlerdir. Bununla birlikte, işletme sektörünün telif hakkı suçlarına karşı 'alternatif' yazılım araçlarını kullanımı artmaktadır.

Kayıt/eğlence şirketleri tarafından zaman içinde kullanılan veya savunulan bazı yazılım tabanlı taktikler telif haklarını korumayı amaçlar:

- Bir **Trojan**, kullanıcıları, indirmeye çalıştıkları telif hakkı korumalı çalışmaları (örneğin bir şarkı) yasal olarak satın alabilecekleri web sitelerine yönlendirir.
- **Donduran yazılımlar**, belirli bir süre bilgisayarları engeller ve korsan içerik indirme konusunda bir uyarı görüntüler.
- **Sabit sürücü taramaları** korsan dosyaları bulur ve siler.
- **Yasaklama**, korsan içeriği indirmeye veya paylaşmaya çalışanlar için İnternete erişimi engeller.

Bu tür önlemlerin bazıları tarafından yasadışı olma potansiyeline sahip olarak görülmektedir.³⁶ Ortaya çıkan soru, bu tür kendi önlemlerini alan şirketlerin yasaları çiğneyip çiğnemedikleridir.

Dijital hakların yönetimi için teknolojiler

Uzun vadeli ve daha yapısal bir yaklaşım olarak, iş sektörü telif hakkı korumalı malzemelere erişimi yönetmek için çeşitli teknolojiler geliştirmiştir. Microsoft, ses dosyalarının, filmlerin ve diğer telif hakkı olan materyallerin indirilmesini yönetmek için dijital haklar yönetimi yazılımı ortaya koymuştur. Benzer sistemler, Xerox (ContentGuard), Philips ve Sony (InterTrust) tarafından geliştirilmiştir.

Telif hakkı koruması için teknolojik araçların kullanımı, WIPO Telif Hakkı Anlaşması ve DMCA'da yasal dayanak bulur. Ayrıca, DMCA, telif hakkıyla korunan malzemelerin teknolojik korumasını önlemeye yönelik etkinlikleri suçlamaktadır.

Meseleler

Var olanı değiştirmek veya yeni telif hakkı mekanizmaları geliştirmek?

BİT ve İnternet gelişmelerinden kaynaklanan derin değişiklikleri yansıtabilecek şekilde telif hakkı mekanizmaları nasıl ayarlanmalıdır? ABD hükümetinin **Fikri Mülkiyet ve Ulusal Bilgi Altyapısı Hakkındaki Beyaz Kitabının**³⁷ önerdiği yanıtlardan birisi, özellikle “fiksasyon”, “dağıtım”, “iletim”, “yayın” kavramlarını temelde “maddesel olmaktan çıkarak” mevcut düzenlemede sadece küçük değişikliklere ihtiyaç duyulmasıdır. Bu yaklaşım, **Fikri Mülkiyet Hakları** (TRIPS) anlaşması ve **WIPO Telif Anlaşması'nın Ticaretle İlgili Etkileri** de dahil olmak üzere başlıca uluslararası telif hakkı anlaşmalarında takip edilmiştir.

Ancak, karşıt görüş yasal sistemdeki değişikliklerin derin olması gerektiğini savunuyor, çünkü dijital çağdaki telif hakkı artık sadece “kopyalamayı önleme hakkını” değil, aynı zamanda “erişimi engelleme hakkını” da ifade etmektedir. Sonuçta, soru, dijital malzemelere erişimi kısıtlamak için her zamankinden daha büyük teknik imkanlarla, telif hakkının korumasının gerekli olup olmadığıdır. Telif hakkı denkleminin ikinci kısmı olan halkın çıkarlarının nasıl korunacağı ortada durmaya devam etmektedir.

Kamu çıkarlarının korunması - telif hakkıyla korunan malzemelerin adil kullanımı

Telif hakkı başlangıçta yaratıcılığı ve buluşu teşvik etmek için tasarlandı. İki unsuru birleştire-

riyordu: yazarın haklarının ve halkın çıkarının korunması. Asıl zorluk, yaratıcılığı, bilgiyi ve küresel refahı arttırmak için halkın telif haklı materyallere nasıl erişebileceğini belirlemektir. Operasyonel olarak konuşursak, korunan malzemelerin “adil kullanımı” kavramı ile kamu çıkarının korunması sağlanır.³⁸

Telif hakkı ve gelişmeler

Telif hakkı başvurusu ne kadar katı olursa, gelişmekte olan ülkeler o kadar etkilenmektedir. İnternet, küresel akademik ve bilimsel değişimlere katılmak için gelişmekte olan ülkelerdeki araştırmacılara, öğrencilere ve diğerlerine güçlü bir araç sunmaktadır. Daha kısıtlayıcı bir telif hakkı rejiminin, gelişmekte olan ülkelerde insan kapasitesinin gelişimi üzerinde olumsuz bir etkisi olabilir. Diğer bir husus, gelişmekte olan ülkelere gelen kültürel ve sanatsal el sanatlarının sayısallaştırılmasıdır. En paradoksal senaryoda, gelişmekte olan ülkeler, sayısallaştırıldıklarında, yeniden paketlenirken ve yabancı eğlence ve medya şirketlerince sahip olduğunda kendi kültürel ve sanatsal miraslarına ödeme yapmayı durdurmak durumunda kalabilirler.

WIPO ve WTO

IPR için iki ana uluslararası rejim bulunmaktadır. WIPO, IPR rejimini Bern ve Paris sözleşmelerine dayanarak yönetmektedir. Bir başka rejim DTÖ tarafından yürütülmekte ve TRIPS’e dayanılmaktadır. Uluslararası IPR koordinasyonunun WIPO’dan DTÖ’ye kaydırılması, hakların korunmasını güçlendirmek için, özellikle uygulama alanında gerçekleştirilmiştir.

Bazı gelişmekte olan ülkeler bu gelişme ile ilgilenmiştir. Endişeleri, DTÖ’nün sıkı uygulama mekanizmalarının, gelişmekte olan ülkelerin manevra alanını ve kalkınma ihtiyaçlarını uluslararası IPR’nin korunmasıyla dengeleme olasılığını azaltabileceği yönündedir. Şimdiye kadar, DTÖ ve TRIPS’in ana odağı, farmasötik ürünler için IPR’nin çeşitli yorumlamaları olmuştur. Tartışmaların IPR ve İnternete uzanması muhtemeldir.

www.igbook.info/copyright

Ticari markalar

Ticari marka, bir şirketi veya ürünü temsil eden kullanımıyla yasal olarak tescil edilmiş veya kurulmuş bir sembol veya kelimedir. Ticari markalar, genellikle alan adlarının tescilinden dolayı İnternet ile ilgilidir. İnternet gelişiminin ilk evresinde, alan adlarının tescili ilk gelene ilk servis esasına göre yapıldı. Bu, şirketlerin alan adı isimlerini satın alma ve daha sonra daha yüksek bir fiyata satma uygulaması olan siber baskıya yol açmıştır.

Bu durum, iş sektörünü, ticari markaların korunması sorununu İnternet yönetişimi reformunun merkezine yerleştirmeye zorladı ve 1998’de ICANN’in kurulmasına yol açtı. **İnternet Adları ve Adresleri Yönetimi Beyaz Kitabında**, ABD hükümeti alanı adları alanında ticari markaların korunmasına yönelik bir mekanizmanın geliştirilmesi ve uygulanması çağrısında bulundu.³⁹ Oluşturulmasından kısa bir süre sonra, ICANN UDRP’yi tanıttı.⁴⁰

Alan adı, ‘.doctor’, ‘.lawyer’, ‘.berlin’ gibi yeni gTLD’ler tanıtılarak genişletildiğinde ticari marka endişeleri daha da netleşti. Böyle bir tartışmaya örnek olarak ‘.amazon.’ gTLD başvurusu verilebilir. Amazon İnternet şirketi, bu isim için ticari marka sahibi olarak “.amazon.”u tescil etmiştir. Amazon havzasındaki ülkeler, ICANN’ın GAC’ine itiraz etmiş, bu adın bölge için önemli olan bir coğrafi bölgeye atıfta bulunduğunu ve şirketin gTLD’ye münhasır kullanım için tahsis edilmemesi gerektiğini savunmuştur. GAC tavsiyelerine dayanarak, ICANN Kurulu başvuruyu Mayıs 2014’te reddetmiştir, ancak kararın ardından ICANN’ın Bağımsız İnceleme Süreci (IRP) aracılığıyla Amazon tarafından itiraz edilmiştir. Ekim 2016 itibarıyla, dava halen açıktır. IRP devam ederken ve geçici olarak Şubat 2017 Mart 2017 için planlanan bir duruşma yapılmıştır.⁴¹

www.igbook.info/trademarks

Patentler

Bir patent, patent sahibine, başkalarını buluşu yapma, kullanma veya satma dışında bırakma hakkını vermiştir. Geleneksel olarak, bir patent esas olarak teknik veya üretim yapısına sahip yeni bir işlemi veya ürünü korur. Sadece son zamanlarda yazılım için patent verilmiştir.

VoIP, NesNet, vs. alanındaki teknolojiler gibi İnternet teknolojilerinin sürekli evrimleşmesiyle, gittikçe daha fazla şirket patent başvurusunda bulunmaktadır. Bu, özellikle, daha fazla patent kaydının, şirketler arasında çok miktarda para içeren daha fazla davaya neden olduğu ABD’deki durumdur. Örnek olarak, Eylül 2016’da, 2010’da başlayan bir davada, ABD’nin Teksas eyaletinde bir hakim, Apple’a başka bir ABD şirketine 302,4 milyon dolar ödemesine hükmetmiştir.⁴²

Bazı patentler iş süreçleri için verilmiş olup, bazıları da İngiliz Telekom’un 1980’lerde kayıtlı olduğu köprü metni bağlantılarında patent için lisans ücreti talep etmesi gibi tartışmalıydı. Ağustos 2002’de dava reddedildi.⁴³ British Telecom bu davayı kazanmış olsaydı, İnternet kullanıcıları oluşturulan ya da kullanılan her köprü metni için bir ücret ödemek zorunda kalacaklardı.

Yazılıma patent verilmesi Avrupa ve diğer bölgelerde oldukça karmaşık bir konudur. Avrupa Patent Ofisinin açıkladığı gibi, ‘Avrupa Patent Sözleşmesi uyarınca’, patent “olduğu” iddia edilen bir bilgisayar programı patentli bir buluş değildir [...]. Bir bilgisayar tarafından uygulanan bir buluş için verilecek bir patent için, teknik bir sorunun özgün ve “kesin olmayan bir biçimde” çözülmesi gerekir.⁴⁴

İş hukuku

İnternet çalışma biçimimizi değiştirdi. Tele-çalışma nosyonu önem kazanmış, geçici ve kısa vadeli çalışmaların sayısı artmıştır. ‘Pematemp’ terimi, düzenli olarak gözden geçirilen kısa vadeli sözleşmelerde uzun süre tutulan çalışanlar için kullanılmıştır. Bu, işgücünün sosyal olarak daha düşük düzeyde korunmasını yol açar (Şekil 18).

İsteğe bağlı emek ve bağımsız işçi modelleri gibi yeni emek modelleri, Uber, Amazon ve diğer internet şirketleri tarafından şekillendirilen iş modellerinde daha yeni bir gelişmedir. Bu süreçte

yeni modeller birkaç soru ortaya çıkardı. Örneğin, Uber sürücüleri bağımsız yükleniciler mi yoksa Uber çalışanları mı? Bu, ABD eyaletlerinde farklı görüşlere neden oldu: California⁴⁵ ve Oregon'daki⁴⁶ otoriteler sürücüleri Uber çalışanları olarak görüyor, Florida⁴⁷ ise bunları müteahhit olarak nitelendiriyor.



Şekil 18. İş Hukuku

İş hukuku alanında, önemli konulardan biri işyerinde mahremiyet meselesidir. Bir işverenin, çalışanların İnternet kullanımını (e-posta mesajlarının içeriği veya web sitesine erişim gibi) izlemesine izin veriliyor mu? Hukuk bu alanda giderek gelişmektedir.

2007 Avrupa İnsan Hakları Mahkemesi'nin (AİHM) verdiği karar, bir çalışanın çalışma yerinde e-posta veya İnternet kullanımının izlenmesinin çalışanın insan haklarını ihlal ettiğini beyan ederken,⁴⁸ aynı mahkeme tarafından 2016 tarihli bir karar, işverenlerin çalışanların mesai saatleri içerisinde yapılan özel iletişimini okuyabilir. Mahkemenin Bărbulescu'nun Romanya'ya açtığı (Ocak 2016) davadaki gerekçesi, bir işverenin çalışanların mesai saatlerinde mesleki görevlerini tamamladığını doğrulamak istemesinin makul olmasıydı. Yine de, işveren herhangi bir izleme faaliyeti hakkında önceden bildirimde bulunmalıdır. Danimarka'da mahkemeler, bir çalışanın özel e-postalar göndermek ve cinsel yönelimli sohbet web sitesine erişmek için görevden alınmalarını içeren bir davayı görüşmüştür. Mahkeme, işverenin İnternetin gayri resmi kullanımını

yasaklayan bir İnternet kullanım politikası bulunmadığı için işten çıkarmanın yasal olmadığına hükmetmiştir. Bărbulescu'nun Romanya'ya açtığı dava konusundaki AİHM kararı ayrıca bir politikanın gerekliliğini de vurgulamaktadır: 'E-posta kullanımı, anında mesajlaşma, sosyal ağlar, bloglama, sörf yapma ve web kullanımıyla ilgili özel kurallar dahil olmak üzere, işyerinde kapsamlı bir İnternet kullanım politikası uygulanmalıdır. Politika, her bir şirketin ihtiyaçlarına ve özellikle de şirket altyapısının her bir sektörünün ihtiyaçlarına göre uyarlanabilse de, çalışanların hak ve yükümlülükleri, izlemenin nasıl yapıldığı, verilerin nasıl güvence altına alındığı, kullanıldığını ve imha edildiğini ve bunlara kimlerin erişimi olduğunu gösterecek şekilde internet'in nasıl kullanılacağına ilişkin şeffaf kurallarla açıkça belirtilmelidir.⁴⁹

Sürekli artan sosyal ağ kullanımıyla ortaya çıkan ek bir endişe konusu özel hayatla çalışma hayatı arasındaki sınırlamadır. Son vakalar,⁵⁰ çalışanların sosyal paylaşım siteleri üzerindeki davranışlarının ve yorumlarının, işyeri ve çalışanlardan işverenlerin strateji ve ürünlerine kadar kişisel (ve özel) görüşler olarak kabul edilen, ancak şirketlerin ve meslektaşlarının imajını ve itibarını önemli ölçüde etkileyebilecek çeşitli konulara değinebileceğini göstermiştir.

İş hukuku geleneksel olarak ulusal bir konudur. Bununla birlikte, genel olarak küreselleşme ve özellikle de İnternet, işgücü sorunlarının uluslararasılaşmasına yol açmıştır. Yabancı şirketler için çalışan ve dünya çapında çalışma ekipleriyle etkileşime giren bireylerin sayısı arttıkça, uluslararası uygun düzenleme mekanizmalarına artan bir ihtiyaç duyulmaktadır. Bu özellik, 47. paragrafta, BİT işgücü piyasası alanındaki tüm ilgili uluslararası normlara saygı gösterilmesini isteyen **WSIS İlkeleri Bildirgesi**'nde kabul edildi.⁵¹

www.igbook.info/labourlaw

Aracılar

Aracılar⁵² İnternet işlevselliğini sağlamada hayati bir rol oynamaktadır. Bunlar arasında (son kullanıcılar arasındaki bağlantıyı sağlayan) ISS'ler ve ayrıca çevrimiçi barındırma, arama motorları ve sosyal medya platformları gibi servis sağlayıcılar bulunur.

Çevrimiçi içeriğin iletimini ve kullanılabilirliğini kolaylaştırmadaki rolleri göz önüne alındığında, araçlardan, telif hakkı ihlali, spam ve unutulma hakkı gibi alanlarda yasal kuralların uygulanmasına yardımcı olmaları giderek daha fazla talep edilmektedir. Bu durum, araçların erişimi kolaylaştırdıkları çevrimiçi içerikten sorumlu olup olmadıklarına dair kapsamlı tartışmalara yol açmıştır.

Ulusal düzeyde, ISS'ler genellikle hükümetlerin ve kolluk kuvvetlerinin çevrimiçi olarak yasal kuralları uygulamalarının en doğrudan yoludur.

Çevrimiçi içeriğe ve arama motorlarının ve sosyal medya platformlarının operatörlerine ev sahipliği yapan kişiler, genellikle içerik için kanallar veya içerik ile İnternet kullanıcıları arasında köprü görevi görür. Bazıları bölgesel merkezlere sahip olanlar olmak üzere bir ülkede merkezi olmasına rağmen, bunların erişim ve kullanıcı tabanlarının küresel olması muhtemeldir ve sonuç olarak birçok ülkede yargı yetkisine maruz kalmaktadırlar.

Aracı sorumluluğu genellikle IGF toplantılarında ve diğer forumlarda tartışılmaktadır. CoE, roller ve sorumluluklarla ilgili bir dizi teklif hazırlanması görevini üstlenen İnternet Aracı Kurumları hakkında bir Uzmanlar Komitesi (MSI - NET) kurmuşken, OECD, İnternet politikaları oluşturma konusundaki 14 ilkesi⁵³ arasında arabulucuların rolünü belirlemiştir. UNESCO, İnternet aracılarının içerik ve İnternet kullanıcılarının yazarları arasında oynadıkları arabuluculuk rolünün yanı sıra ifade özgürlüğü ve gizlilik gibi ilgili temel haklar üzerindeki etkisini araştırmıştır.⁵⁴

Meseleler

Telif hakkı ihlali için aracı sorumluluğu

Genel olarak, arabuluculuk sorumluluğuyla ilgilenen yasal çerçeveler, ihlalin farkında değilse, telif haklarını ihlal eden materyallerin barındırılmasından bir İnternet aracısının sorumlu tutulamaz. Bu, örneğin, DMCA ve AB direktifinin,⁵⁵ servis sağlayıcısını kullanıcılar doğrultusunda iletilen veya saklanan bilgiler için sorumluluktan muaf tutan yaklaşımıdır.

Çeşitli yasal sistemler arasındaki temel fark, aracı kurumun barındırdığı materyalin telif haklarına aykırı olduğunun farkına vardıkdan sonra yapılan yasal işlemlerde yatmaktadır. ABD ve AB hukuku, hizmet sağlayıcıların “ihbarda ve etkisiz hale getirme” işlemi yapmalarını talep eder.⁵⁶ Japon yasaları, malzemenin kullanıcıya çıkarılması talebiyle ilgili şikayette bulunma hakkı sağlayan İhbar - Bildirim - İhbar - Etkisiz Hale Getirme prosedürü aracılığıyla daha dengeli bir yaklaşım benimsemiştir. Her iki çözüm de, yasal yaptırımlara karşı güvenli oldukları için aracılara bir miktar rahatlık sağlar, ancak aynı zamanda potansiyel olarak onları içerik hakimlerine⁵⁷ dönüştürür ve tartışmalı içerik başka bir çevrimiçi konuma taşınabileceği için sorunu yalnızca kısmen çözer.

Aracılara sınırlı sorumluluk koyma yaklaşımı, genel olarak hukuk yoluyla desteklenmiştir. İSS'lerin telif hakkı yasalarını ihlal eden materyalleri barındırma sorumluluğundan kurtulduğu en önemli durumlardan bazıları Scientology Davası (Hollanda),⁵⁸ RIAA'nın Verizon'a açtığı dava (ABD),⁵⁹ SOCAN'ın CAIP'e açtığı dava (Kanada)⁶⁰ ve Scarlet'in SABAM'a açtığı davadır (Belçika).⁶¹ GS Media BV'nin Sanoma Media Netherlands BV'ye ve Diğerlerine açtığı davaları için Eylül 2016'da CJEU tarafından yayınlanan daha ayrıntılı bir karar, telif haklarını ihlal eden materyallere bağlanan web sitelerinin operatörlerinin, bunu bilmeleri veya materyalin bir ihlal teşkil ettiğini makul bir şekilde bilebilmeleri ihtimali halinde telif hakkı ihlalden suçlu bulunabileceğini ifade etmektedir. Mahkemeye göre, ‘finansal kazancın peşinde’ bağlantılar sağlanmışsa, işletmecilerin ihlaller hakkında bilgi sahibi olacağı tahmin edilebilir.⁶²

Bununla birlikte, son yıllar, son kullanıcılar ve İnternet içeriği arasındaki kapı bekçileri, erişimi kontrol etmek için en iyi pozisyona yerleştirdiklerinden, telif hakkı meseleleriyle ilgili olarak araçlar üzerinde artan bir baskıya şahit olmuştur. Bu argüman, ISS'leri telif hakkı ihlali şüpheleri durumunda müdahale etmeye zorlayan Fransa'daki Hadopi Yasası⁶³ gibi yasal hükümlerin desteklenmesi yönünde yorumlanmıştır.

Aracıların içerik politikasındaki rolü

Artan resmi baskılar karşısında, içerik barındırma hizmetleri sağlayıcıları olan ISS'ler ve arama motorları ve sosyal ağ platformlarının işletmecileri isteksizce olsa da, içerik politikasına (örneğin, hakaret içeren veya sahte içerik) yavaş yavaş giderek artan biçimde dahil olmaktadır. Bunu yaparken, iki olası yolu izlemeleri gerekebilir. Birincisi hükümet düzenlemesini uygulamaktır. İkincisi, öz düzenlemeye dayalı olarak, araçların kendilerinin neyin uygun olduğuna karar vermeleridir. Bu, hükümetlerin sorumluluklarını devralan araçlarla içerik kontrolünü özelleştirme riskini taşımakta, ancak teknolojinin hızla ilerlemesini sağlamak için esnek yaklaşımlar benimseme avantajını taşımaktadır. Bu özellikle çevrimiçi çocuk koruma alanında önemlidir.

Hukuk mahkemeleri giderek aracı kurumlara kurallar koymaktadır. 2013 yılında AİHM, Estonya mahkemeleri tarafından Delfi haber portalının web sitesinde yayınlanan rahatsız edici yorumlardan sorumlu olduğunu belirten bir kararı onayladı.⁶⁴ Haziran 2015'te, AİHM Büyük Dairesi 2013 kararını doğruladı: Estonya mahkemelerinin kararı haklı ve orantılıydı; çünkü yorumlar aşırı ve ticari olarak çalışan ve profesyonelce yönetilen haber portalı Delfi tarafından yayınlanan bir makaleye tepki olarak yayınlanmıştı.⁶⁵ (Ancak bu karar, İnternet tartışma forumu, ilan tahtası veya sosyal medya platformu gibi üçüncü tarafların paylaşılabilceği diğer çevrimiçi alanlarla ilgili değildir.)

İstenmeyen postadan korunma politikasında araçların rolü

ISS'ler yaygın olarak spam karşıtı girişimlerle ilgili birincil kurumlar olarak görülmektedir. Genellikle, ISS'lerin spam'i azaltmak için teknik filtreleme veya istenmeyen posta önleme politikasını uygulama yoluyla kendi girişimleri bulunmaktadır. 2006 yılına ait bir ITU raporu, ISS'lerin spam'den sorumlu olması gerektiğini ve iki ana hükümle birlikte spam karşıtı bir davranış kodu önerdiğini söylemiştir:

- Bir ISS kullanıcılarının spam yapmasını yasaklamalıdır.
- Bir ISS, benzer bir davranış kuralını kabul etmeyen bir ISS ile eş olmamalıdır.⁶⁶

Spam sorunu, ISS'leri yeni zorluklara maruz bırakmıştır. Örneğin, Verizon'un spam karşıtı filtrelemesi, yasal e-postalarını almayan kullanıcılar için rahatsızlık yaratan meşru mesajları engellediği için bir davaya yol açmıştır.⁶⁷ Kuşkusuz, ISS'ler tarafından benimsenen özerk ve ortak düzenleme yaklaşımları, uluslararası işbirliği ve karmaşık filtrelerin kullanımı ile birlikte spam politikasının etkisi azalmıştır.

www.igbook.info/intermediaries

Son notlar

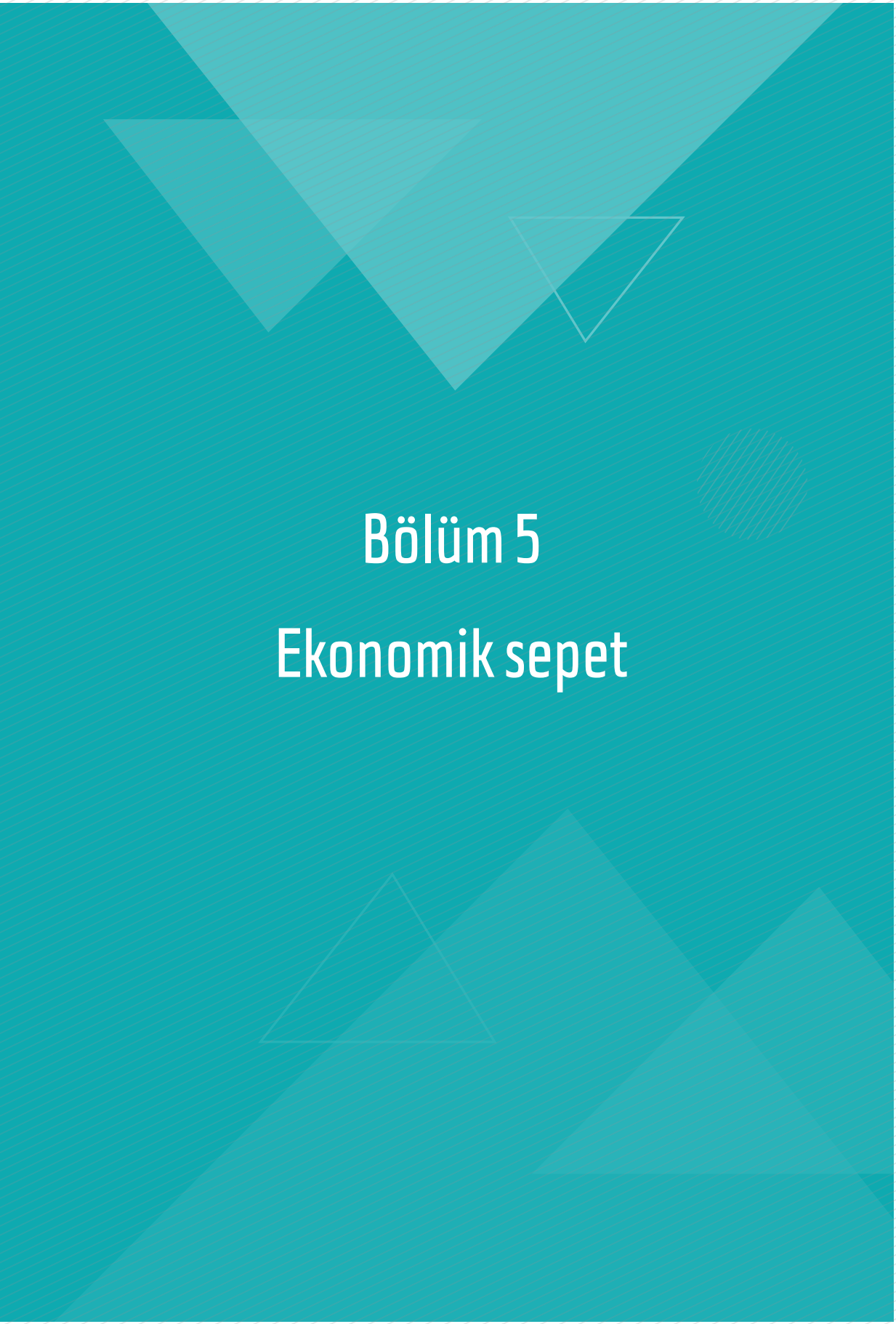
- 1 Gerçek hukuk yaklaşımı konusundaki ilk argümanlardan bazıları Hakim Frank Easterbrook tarafından sağlanmıştır. Sanığa şöyle demiştir: ‘Eve git; siber kanun yoktur.’ ‘Siber Yasa ve At Yasası’ adlı makalesinde, atlar çok önemli olmasına rağmen, Atın Yasası olmadığını iddia etmektedir. Hakim Easterbrook, sözleşmeler, sorumluluk vb. gibi temel yasal araçlara odaklanma gereğinin olduğunu savunmaktadır. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles [Erişim 24 Ekim 2016]. Easterbrook’un argümanı, At Hukuku: What Cyberlaw Might Teach isimli eserinde Lawrence Lessig’in dediği: Ciber Yasa ne öğretebilir de dahil olmak üzere çeşitli tepkilere neden oldu. http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF [Erişim 24 Ekim 2016]. Further discussion of the real-law and cyberlaw approaches can also be found on The Oxford Comma blog: Shaping Internet Governance: Tensions Between ‘Real’ and ‘Cyber’ Laws. <http://wizardsqu1rrel.blogspot.com/2014/01/shaping-internet-governance-tensions.html> [Erişim 24 Ekim 2016].
- 2 United Nations (2013) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf> [Erişim 29 Ekim 2016].
- 3 United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf> [Erişim 27 Ekim 2016].
- 4 United Nations General Assembly (2014) Resolution A/69/166. The right to privacy in the digital age. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 [Erişim 29 Ekim 2016]. United Nations Human Rights Council. Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [Erişim 29 Ekim 2016].
- 5 NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. <https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses> [Erişim 24 Ekim 2016].
- 6 Örneğin, yönetmeliklere göre ‘Üye Devlet tarafından yetkilendirilen veya tanınan, kamuya uluslararası telekomünikasyon hizmetlerini kurmak, işletmek ve uğraşmak için faaliyet gösteren kuruluşlar için uygulanacak yeni hüküm’ ISR’leri de dahil ederek kapsamını genişletiyor gibi görünmektedir. Tartışma ayrıca ağ güvenliği ve istenmeyen elektronik iletişim ile ilgili hükümlerin getirilmesini de içermektedir. Daha geniş bir siber güvenlik kavramıyla ilişkilendirildiklerinden (e-postalar bağlamında spam ile ilgili olarak da dahil olmak üzere), bu hükümlerin yalnızca geleneksel telekomünikasyonlara uygulanabilir olduğunu (ve İnternete değil) yorumlamanın zor olduğu iddia edilmiştir. Bu tür hükümlerin farklı yorumlarına ek olarak, (1988 ITR’leri karşılaştırıldığında değişmeden kalan) telekomünikasyon tanımının kendisi, bazılarının İnternet üzerinden yapılan iletişimlere de kapsıyor gibi görülmektedir: ‘işaretlerin, sinyallerin iletilmesi, yayılması veya alınması, tel, radyo, optik veya diğer elektromanyetik sistemlerle yazı, görüntü ve ses veya herhangi bir nitelikteki zeka gibi’.
- 7 Ago R (1956) Science juridique et droit international. Recueil des Cours Academie de Droit International (RCADI), 1956-II, 855–954, La Haye
- 8 Vienna Convention on the Law of Treaties. <http://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf> [Erişim 28 Ekim 2016].
- 9 Brownlie I (1999) Principles of Public International Law, 5th Ed. Oxford: Oxford University Press, p. 513.

- 10 Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyber- space Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. <http://www.jstor.org/discover/10.2307/4068795?uid=3738216&uid=2&uid=4&sid=21103388060741> [Erişim 28 Ekim 2016].
- 11 Among the most important resources in this field is the Princeton Principles on Universal Jurisdiction (2001). <http://www1.umn.edu/humanrts/instree/princeton.html> [Erişim 28 Ekim 2016].
- 12 Malanczuk P (1997) Akehurst's Modern Introduction to International Law. London: Routledge, p. 113.
- 13 CJEU (2013) Judgement of the Court in Case C-170/12: Peter Pinckney v KDG Mediatech AG. <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-170/12&td=ALL> [Erişim 29 Ekim 2016].
- 14 CJEU (2011) Judgement of the Court in Joined Cases Cases C-509/09 and C-161/10: eDate Advertising GmbH v X, and Olivier Martinez, Robert Martinez v MGN Limited. <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-509/09&td=ALL> [Erişim 29 Ekim 2016].
- 15 EDRI-gram (2006) French anti-hate groups win case against Yahoo! <http://edri.gn.apc.org/edriagram/number4.1/yahoocase> [Erişim 24 Ekim 2016].
- 16 İnternet içeriği ile ilgili dünya dışı yargı yetkisi içeren davalara genel bir bakış için, bkz. Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. Connecticut Journal of International Law, 20, 199. <http://ssrn.com/abstract=637961> [Erişim 24 Ekim 2016].
- 17 Nispeten benzer bir durum, soykırımın mevcudiyetini sorgulayan materyali bir Avusturya merkezli bir web sitesinde yayınlanmış Avustralya'lı ve aynı zamanda eski bir Alman vatandaşı olan Fredrick Toben'e karşı, Federal Adalet Divanı davasıydı. http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html [Erişim 24 Ekim 2016].
- 18 Commission Nationale de l'Informatique et des Libertés (2015) Right to delisting: Google informal appeal rejected. <https://www.cnil.fr/fr/node/15814> [Erişim 11 Ekim 2016].
- 19 CJEU (2015) Judgement of the Court in Case C-362/14: Maximillian Schrems v Data Protection Commissioner. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015> [Erişim 21 Ekim 2016].
- 20 United States Court of Appeals for the Second Circuit (2016) Decision in the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation: Microsoft Corporation v USA. <http://www.ediscoverylaw.com/wp-content/uploads/2016/07/In-re-Matter-of-a-Warrant.pdf> [Erişim 24 Ekim 2016].
- 21 Fransa'daki mahkeme emri için bkz. <http://www.cottineau.net/wp-content/uploads/2016/02/face-book-jugement-cour-appel-paris-12-fevrier-2016.pdf> [Erişim 12 Ekim 2016].
- 22 Yaron O (2016) Israeli judge approves \$400 million class action against Facebook for violating privacy. Haaretz, 17 June. <http://www.haaretz.com/israel-news/business/1.725512> [Erişim 12 Ekim 2016].
- 23 Tartışmalı konulara örnek olarak şunlar dahildir: ırkçı içerik, pornografi, çevrimiçi kumar, tütün reklamı ve uyuşturucu satışı.
- 24 UNCITRAL (1958) The New York Convention. http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html [Erişim 24 Ekim 2016].
- 25 UNCITRAL (1985) Model Law in International Commercial Arbitration. http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html [ac- cessed 24 Ekim 2016].
- 26 WIPO (no date) Domain Name Dispute Resolution. <http://www.wipo.int/amc/en/domains/> [Erişim 25 Ekim 2016].

- 27 European Commission (2016) Settling consumer disputes online. http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adr-odr.factsheet_web.pdf [Erişim 25 Ekim 2016].
- 28 Google (2016) Transparency Report. European privacy requests for search removals. <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> [Erişim 29 Ekim 2016].
- 29 WIPO (no date) WIPO Copyright Treaty. <http://www.wipo.int/treaties/en/ip/wct/> [Erişim 1 Kasım 2016].
- 30 Office of the United States Trade Representative (no date) The Trans-Pacific Partnership. <https://ustr.gov/tpp/> [Erişim 1 Kasım 2016].
- 31 US Congress (1998) Digital Millennium Copyright Act. <http://www.copyright.gov/legislation/hr2281.pdf> [Erişim 1 Kasım 2016].
- 32 US Congress (2011) Stop Online Piracy Act. <https://www.congress.gov/bill/112th-congress/house-bill/3261> [Erişim 24 Ekim 2016].
- 33 US Congress (2011) Protect IP Act. <https://www.congress.gov/bill/112th-congress/senate-bill/968> [Erişim 24 Ekim 2016].
- 34 Anti-Counterfeiting Trade Agreement (2011) http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf [Erişim 24 Ekim 2016].
- 35 Sivil haklar savunucusu bir grup olan La Quadrature du Net Hadopi yasasındaki gelişmeleri yakından takip etmekte ve ACTA hakkında kapsamlı bir dosya hazırlamaktadır. <http://www.laquadrature.net/en/ACTA> [Erişim 25 Ekim 2016]. ABD aleyhine protestolar için bkz. Vijayan J (2012) Protests against SOPA, PIPA go viral. Computerworld, 18 January. http://www.computerworld.com.au/article/412655/protests_against_sopa_pipa_go_viral/ [Erişim 25 Ekim 2016].
- 36 Sorkin AR (2003) Software bullet is sought to kill musical piracy. New York Times, 4 May. Available at <http://www.nytimes.com/2003/05/04/business/04MUSI.html> [Erişim 25 Ekim 2016].
- 37 US Patents and Trademark Office (no date) Intellectual Property and the National Information Infrastructure. <http://www.uspto.gov/web/offices/com/doc/ipnii/> [Erişim 25 Ekim 2016].
- 38 Adil kullanım kavramının açıklaması ve örnekleri için bkz. The UK Copyright Service (no date) Copyright Law fact sheet P-09: Understanding Fair Use. http://www.copyrightservice.co.uk/copyright/p09_fair_use [Erişim 25 Ekim 2016].
- 39 NTIA (1998) Statement of Policy on the Management of Internet Names and Addresses. <https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses> [Erişim 1 Kasım 2016].
- 40 For a comprehensive survey of the main issues involving UDRP, please consult WIPO (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) <http://www.wipo.int/amc/en/domains/search/overview2.0/> [accessed 25 Ekim 2016].
- 41 For more details about the .amazon case, consult Murphy K (2016) Amazon files appeal on rejected .amazon domain. The Register, 3 March 2016. <http://domainincite.com/20105-amazon-files-appeal-on-rejected-amazon-domain> [Erişim 25 Ekim 2016]. For details on the IRP initiated by Amazon, consult ICANN (no date) Amazon EU S.à.r.l. v ICANN (.AMAZON). <https://www.icann.org/resources/pages/irp-amazon-v-icann-2016-03-04-en> [Erişim 25 Ekim 2016].
- 42 Decker S and Robertson D (2016) VirnetX Wins \$302.4 Million Trial Against Apple in Texas. Bloomberg, 30 September. <https://www.bloomberg.com/news/articles/2016-10-01-virnetx-wins-302-4-million-trial-against-apple-in-texas> [Erişim 25 Ekim 2016].
- 43 Loney M (2002) Hyperlink patent case fails to click. CNET, 23 Ağustos. <https://www.cnet.com/news/hyperlink-patent-case-fails-to-click/> [Erişim 25 Ekim 2016].
- 44 European Patent Office (no date) Patents for software? European law and practice. <https://www.epo.org/news-issues/issues/software.html> [Erişim 25 Ekim 2016].

- 45 Somerville H (2015) Former Uber driver was an employee, rules California department. Reuters, 9 September. <http://www.reuters.com/article/uber-tech-california-ruling-idUSL1N11F1KT20150910> [Erişim 29 Ekim 2016].
- 46 Bureau of Labour and Industries of the State of Oregon (2016) Advisory opinion of the Commissioner of the Bureau of Labor and Industries regarding the employment status of Uber drivers. <http://media.oregonlive.com/commuting/other/101415%20Advisory%20Opinion%20on%20the%20Employment%20Status%20of%20Uber%20Drivers.pdf> [Erişim 29 Ekim 2016].
- 47 Ampel C (2015) Florida: Uber drivers are contractors, not employees. Daily Business Review, 4 December. Available at <http://www.dailybusinessreview.com/id=1202743938454/Florida-Uber-Drivers-Are-Contractors-Not-Employees?slreturn=20160929162026> [Erişim 29 Ekim 2016].
- 48 ECHR (2007) Judgement of the Court in the Case Copland v the United Kingdom (Application no. 62617/00). <http://hudoc.echr.coe.int/eng?i=001-79996> [Erişim 29 Ekim 2016].
- 49 ECHR (2016) Judgement of the Court in the Case Bărbulescu v Romania (Application no. 61496/08). <http://hudoc.echr.coe.int/eng?i=001-159906> [Erişim 29 Ekim 2016].
- 50 Bkz: Bkz: Holding R (2011) Can You Be Fired for Bad-Mouthing Your Boss on Facebook? Time U.S., 4 March. <http://www.time.com/time/nation/article/0,8599,2055927,00.html> [Erişim 25 Ekim 2016]. Broughton A et al. (2009) Workplaces and Social Networking. The Implications for Employment Relations. http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf [Erişim 25 Ekim 2016].
- 51 WSIS (2003) Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> [Erişim 29 Ekim 2016].
- 52 OECD'nin araçların çalışma tanımı, aracı kavramı altında bulunan çeşitli hizmet sağlayıcı kategorilerini belirlemeye çalışır: 'İnternet araçları, İnternet'te üçüncü şahıslar arasındaki işlemleri bir araya getirir veya daha da kolaylaştırır. İnternetteki üçüncü şahıslardan kaynaklanan içerik ve ürün ve hizmetlere erişim sağlar, barındırır, iletir ve indeksler ya da üçüncü şahıslara İnternet tabanlı hizmetler sunarlar.' Bkz: OECD (2011) The Role of Internet Intermediaries in Advancing Public Policy Objectives. <http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm> [Erişim 29 Ekim 2016].
- 53 OECD (2011) OECD Council Recommendation on Principles for Internet Policy Making. <http://www.oecd.org/internet/ieconomy/49258588.pdf> [Erişim 10 Ekim 2016].
- 54 MacKinnon R et al. (2014) Fostering Freedom Online. The Role of Internet Intermediaries. UNESCO/Internet Society. <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf> [Erişim 10 Ekim 2016].
- 55 European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 Haziran 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031> [Erişim 25 Ekim 2016]. European Union (2001) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477400249287&uri=CELEX:32001L0029> [Erişim 25 Ekim 2016].
- 56 "Bildirim ve Alma" prosedürü, servis sağlayıcıların söz konusu içeriğin yasallığı ile ilgili bir bildirim veya şikayet almaları durumunda, içeriği kendi yönetimleri altındaki web sitelerinin içeriğinden çıkarma yükümlülüğünü ifade eder.
- 57 Potansiyel yasal yaptırımlarla yüzleşme korkusu nedeniyle, bazı ISS'ler ihlal edilmemiş olsa bile belirtilen içeriğe erişimi kısıtlamayı tercih eder. Detaylar için bkz: For Europe (the Netherlands): Nas S

- (2004) The Multatuli Project ISP Notice & Take Down, Bits of Freedom. <https://www-old.bof.nl/docs/researchpaperSANE.pdf> [Erişim 28 Ekim 2016]. For the USA: Urban J and Quilter L (2006) Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1500&context=facpubs> [Erişim 28 Ekim 2016].
- 58 'Lahey Temyiz Mahkemesi, Scientology Kilisesi'ne karşı, Hollandalı bir yazara ve ISS'sine (XS4ALL) yönelik telif hakkı davasıyla karar vermiştir. Eskiden uygulamacı bir Scientolog olan yazar, gizli kilise belgelerini bir web sitesine yayınladı ve kilise, 1912 tarihli Hollanda Telif Hakkı Yasası kapsamında dava açtı. 1999'da Bölge Mahkemesi, sanıkların lehine karar verdi ve konuşma özgürlüğü endişelerini dile getirdi. Bununla birlikte, bu mahkeme ayrıca ISS'lerin mevcut telif haklarını ihlal edebilecek yazılı materyallerden sorumlu tutulmasına karar vermiştir. Temyiz Mahkemesi ilk kararı onayladı, ancak ikinciyi ters çevirerek ISS'lerin yayınlanan materyallerden sorumlu olmadığını söyledi.' Daha fazla bilgi için bkz. Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. <http://cyberlaw.stanford.edu/packets001638.shtml> [Erişim 25 Ekim 2016].
- 59 Bu dava hakkında daha fazla bilgi için bkz. Electronic Privacy Information Center (2004) RIAA v Verizon. <http://epic.org/privacy/copyright/verizon/> [Erişim 25 Ekim 2016].
- 60 The Supreme Court of Canada rejected the argument of the Society of Composers, Authors and Music Publishers of Canada that Canadian ISPs should pay royalties because some of their customers download copyrighted works (SOCAN vs CAIP). More information <http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html> [Erişim 25 Ekim 2016].
- 61 'SABAM (Belçika kolektif topluluğu - Société belge des auteurs, compositeurs et éditeurs), ISP Scarlet'ın hizmetlerinden geçen tüm gelen ve giden elektronik iletişimler için geliştirilmiş bir filtreleme sistemi kurmasını ve potansiyel olarak yasa dışı iletişimlerini engellemesini istedi. Brüksel Mahkemesi birinci Aşamada, ISS'nin sorumluluğunu reddederken, SABAM'ın iddiasının meşru olduğu ve bir filtreleme sisteminin uygulanması gerektiği sonucuna varmıştır. Scarlet kararı temyiz etmiş ve dava Avrupa Birliği Adalet Divanı'na sevk edilmiştir. Adalet Divanı, kararında, mücerret ve önleyici tedbir olarak filtreleme ve engelleme sisteminin tüm müşterileri için sınırsız bir süre için kullanılmasını, temel hakları, özellikle de gizlilik hakkını, iletişim özgürlüğünü ve bilgi özgürlüğünü ihlal ettiğini belirtmiştir. Ayrıca, ISS'lerin iş yapma özgürlüğünü ihlal etmektedir.' Daha fazla bilgi için bkz. CJEU (2011) Judgement of the Court in Case C-70/10: Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL> [Erişim 25 Ekim 2016].
- 62 CJEU (2016) Judgement of the Court in Case C-160/15: GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker. <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-160/15&td=ALL> [Erişim 25 Ekim 2016].
- 63 2013 yılında, Hadopi Yasası'nın bir kısmı, ihlal eden kişiye İnternet erişimini askıya alma cezası oranı tıstı olduğu için iptal edildi.
- 64 ECHR (2013) Judgement of the Court (First Section) in the Case Delfi AS v Estonia (Application no. 64569/09). <http://hudoc.echr.coe.int/eng?i=001-126635> [Erişim 29 Ekim 2016].
- 65 ECHR (2015) Judgement of the Court (Grand Chamber) in the Case Delfi AS v Estonia (Application no. 64569/09). <http://hudoc.echr.coe.int/eng?i=001-155105> [Erişim 29 Ekim 2016].
- 66 Palfrey J (2006) Stemming the International Tide of Spam. In: ITU (2006) Trends in Telecommunication reforms 2006. http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf [Erişim 29 Ekim 2016].
- 67 Shannon V (2006) The end user: Junk payout in spam case – Technology – International Herald Tribune. The New York Times, 26 April. <http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html> [Erişim 28 Ekim 2016].

The background is a solid teal color. It features several large, semi-transparent geometric shapes: a large inverted triangle at the top left, a smaller inverted triangle at the top right, a circle with diagonal lines on the right side, and several large triangles at the bottom, some pointing up and some pointing down.

Bölüm 5

Ekonomik sepet

EKONOMİK SEPET

Paketlerin nasıl yönlendirileceğini biliyoruz.

Nasıl yapacağımızı bilmediğimiz, doları nasıl yönlendireceğiz.

David Clark – Baş İnternet Protokol Mimarı

David Clark'tan gelen bu alıntı, kar amacı gütmeyen İnternet projesinin temel olarak ABD araştırma hibeleriyle desteklendiği erken İnternet topluluğunun ruhunu yansıtıyor. Ancak, 1990'larda ve 2000'lerin başında, "dolandırıcılık yönelimi" için yeni iş modelleri Silikon Vadisi'nde ortaya çıkmaya başlamıştır.

İnternet yönetimindeki ekonomik meseleler, esas olarak internetin kar amacı gütmeyen bir projeden modern toplumdaki ekonomik büyüme ve ana ticari tesislerden birine kadar evrimi ile ilgilidir. İnternetin ilk günlerinden beri kolaylaştırdığı fikirlerin ve yaratıcılığın akışı, para akışıyla rekabet halinde bulunarak artan bir şekilde kendini bulmuştur. Daha fazla para daha somut iş ve politika menfaatleri gündeme getirmiştir. Yaratıcı 'mavi gökyüzü, ilk İnternet topluluğunun sınırır' yaklaşımı, iş dünyasının 'alt çizgisi' mantığıyla birleşmeye başlamıştır. Yüksek yaratıcılık ve sağlam ekonomik destek arasındaki bu etkileşim, Kaliforniya'daki Bay Area bölgesinde coğrafi olarak odaklanan gerçek bir ekonomik devrimi tetiklemiştir.

Dijital politika hem ekonomik gelişmelerden hem de para akışından etkilenir ve onları etkiler.¹ Ekonomik bir büyüme için etkinleştirici bir dijital politika esastır. Örneğin Silikon Vadisi'ndeki hızlı dijital büyümenin nedenlerinden biri, işlevsel düzenleme sistemidir; bu sistem İnternet şirketlerinin fikri mülkiyetini korumuş ve yatırımı teşvik etmiş, daha fazlasını da yapmıştır. Dijital ekonomi için (olanak sağlayan bir politika ortamı olarak) "analog" takviyelerin önemi, Dünya Bankası tarafından 2016 Dünya Kalkınma Raporu: Dijital Kâr Payları'nda incelenmiştir.²

Dijital politika, İnternet şirketlerinden de etkilenmektedir. Bu şirketler Washington D.C., Brüksel ve Cenevre gibi başlıca dijital politika merkezlerinde özellikle etkin olan güçlü lobicilik araçları geliştirmiştir.

İnternete bağlı ekonomik konulara ilişkin analizimiz, parasal ve parasal olmayan ticari işlemlerin gerçekleştiği dört ana alana odaklanmaktadır:

- **E-ticaret:** İnternet üzerinden yürütülen geleneksel ticari faaliyetler.
- **İnternet VERİ ekonomisi:** Yeni reklam tabanlı iş modeli.
- **İnternet ERİŞİM ekonomisi:** İnternet çağında telekomünikasyon endüstrisi.
- **E-bankacılık, e-para, ve sanal dövizler.**

Ayrıca, ekonomiyle ilgisi olan alaka diğer iki politik konusuna bakmaktayız: tüketicinin korunması ve vergilendirilmesi.

E-ticaret

E-commerce has been one of the main engines driving the growth of the Internet over the past 15 years. The importance of e-commerce is illustrated by the title of the document that initiated the reform of Internet governance and paved the way towards the creation of ICANN: the 1997 [Framework for Global Electronic Commerce](#),³ which states that ‘the private sector should lead’ the Internet governance process and that the main function of this governance will be to ‘enforce a predictable, minimalist, consistent, and simple legal environment for commerce’. E - ticaret, İnternetin büyümesini 15 yıl boyunca yönlendiren ana motorlardan biri olmuştur. E-ticaretin önemi, İnternet yönetişimi reformunu başlatan ve ICANN’ın oluşturulmasına giden yolu hazırlayan belgenin başlığında gösterilmiştir. Bu da, internet yönetişimi sürecine ‘özel sektörün öncülük etmesi’ gerektiğini ve ve bu yönetişimin temel işlevinin ‘ticaret için öngörülebilir, minimalist, tutarlı ve basit bir yasal ortamın uygulanması’ olacağını belirten 1997 [Küresel Elektronik Ticaret Çerçevesi](#)’dir.

Günümüzde, e-ticaretin bireyler ve işletmeler üzerindeki etkisi büyük ölçüde artmaktadır. E-ticaret, tüketiciler için çevrimiçi alışverişin rahatlığı, esneklik ve farklı pazarlara erişim kolaylığı ve çevrimiçi bankacılık ve daha az zaman alan e-ödeme işlemleri gibi sayısız avantajlar sağlamıştır. İş açısından bakıldığında, e-ticaret tedarik zinciri yönetimini etkilemiş ve şirketlerin online reklamcılık ve pazarlama ve diğer yollarla müşterileriyle daha kolay bir şekilde ulaşmalarını sağlamıştır. Bununla birlikte, işletmeler daha zorlu bir rekabetle karşı karşıya kalmış ve bir çevrimiçi pazara hizmet ederken yeni karmaşıklıklar eklenmiştir.

Tanım

E-ticaret için bir tanım seçiminin birçok pratik ve yasal çıkarımı vardır. Belirli bir işlemin vergi ve gümrük düzenlemeleri gibi e-ticaret olarak sınıflandırılmasına bağlı olarak belirli kurallar uygulanır.

ABD hükümeti için, geleneksel ticareti e-ticaretten ayıran kilit unsur, mal veya hizmet satmaya yönelik çevrimiçi taahhüttür. Bu, çevrimiçi olarak sonuçlanan herhangi bir ticari anlaşmanın, alışverişin gerçekleşmesi teslimatın fiziksel olarak yapılmasını içerse bile, bir e-ticaret işlemi olarak kabul edilmesi gerektiği anlamına gelir. Örneğin, Amazon.com üzerinden bir kitap satın almak, kitap genellikle geleneksel posta yoluyla teslim edilmekle birlikte bir e-ticaret işlemi olarak kabul edilir. DTÖ, e-ticareti daha kesin olarak şu şekilde tanımlamaktadır: “mal ve hizmetlerin elektronik yollarla üretimi, dağıtımı, pazarlanması, satışı veya teslimi”.⁴ AB’nin e-ticarete yaklaşımı, ‘normal olarak ödeme için kullanılan herhangi bir hizmeti, uzaktan, (dijital sıkıştırma dahil) verilerin işlenmesi ve depolanması ve hizmetin faturasının bireysel talep üzerine elektronik yöntemlerle sunmayı kapsayan “bilgi toplumu hizmetleri” ile ilgilidir’.⁵

E-ticaret birkaç farklı şekildedir:

- [İşletmeden tüketiciye \(B2C\)](#) - en bilinen e-ticaret türüdür (örneğin, Amazon.com).
- [İşletmeden İşletmeye \(B2B\)](#) - B2C pazarının iki katından fazlasını temsil eden bu tür ekonomik olarak en yoğun olanıdır.⁶
- [İşletmeden hükümete \(B2G\)](#) - kamu alımları politikası alanında son derece önemlidir.

- Tüketiciden tüketiciye (C2C) - örneğin, eBay açık artırmaları.

Birçok ülke e-ticaret için yasal çerçeveler geliştirmektedir. Dijital imzalar, çevrimiçi anlaşmazlıkların çözümü, siber suç, tüketicinin korunması ve elektronik hizmetlerin vergilendirilmesi gibi çeşitli alanlarda yasalar kabul edilmiştir. Uluslararası düzeyde, artan sayıda girişim ve rejim e-ticaret ile ilgilidir.

DTÖ ve e-ticaret

Modern küresel ticaretteki kilit politika oyuncusu olarak DTÖ, uluslararası ticareti düzenleyen bir anlaşma sistemi kurmuştur. Başlıca anlaşmalar, mal ticaretiyle ilgili **Genel Tarifeler ve Ticaret Anlaşması** (GATT),⁷ **Hizmet Ticaretinde Genel Anlaşma** (GATS)⁸ ve **TRIPS**'dir.⁹ Bu çerçevede DTÖ, telekomünikasyonun serbestleşmesi, IPR ve BİT gelişiminin bazı yönleri dahil olmak üzere pek çok ilgili e-ticaret meselesini düzenlemektedir. E-ticaret, aşağıdaki DTÖ faaliyetlerinde ve girişimlerinde yer almaktadır:

- 1998'de tanıtılan elektronik yayınlarla ilgili gümrük vergileri üzerine geçici bir moratorium, tüm e-yayınların DTÖ üyesi ülkeler arasındaki gümrük vergilerinin ücretsiz olmasını sağlamıştır.¹⁰
- 1998 yılında kurulan DTÖ Elektronik Ticaret Çalışma Programı, DTÖ organlarının e-ticaretle ilgili alanlarda sorumluluklarını ortaya koymaktadır.¹¹
- Elektronik işlemlerle ilgili davaları, diğerlerinin yanında ele alan bir uyuşmazlık çözümü mekanizması. (Bir örnek, e-ticaretin özellikle ilgili olduğu ABD/Antigua Çevrimiçi Kumar davasıdır.¹²)

E-ticaret, DTÖ'nün ikincil diplomatik öncülüğüne dayanmasına rağmen, çeşitli inisiyatifler ortaya çıkmış ve daha sonra tartışılanlar da dahil olmak üzere çeşitli kilit konular tespit edilmiştir.

E-ticaret işlemleri (GATS tarafından düzenlenmiş) hizmetler veya (GATT tarafından düzenlenmiş) mallar altında mı sınıflandırılmalıdır?

Birçok e-ticaret işleminin ikili bir niteliği vardır. Dijital günlerin başlarında, ana ikilem, bir (somut) CD'de mi ya da (soyut) internet üzerinden teslim edildiğine bağlı olarak, müziğin bir ürün mü yoksa hizmet mi olarak sınıflandırılması gerektiği idi? Sonuçta, aynı şarkı teslimat ortamına bağlı olarak farklı ticaret statüsünde olabilir (ve farklı gümrük ve vergilere de tabi olabilir). Sınıflandırma sorunu, aynı zamanda (çevrimiçi sözleşmeler, yazılımların dağıtımı gibi) somut olmayan unsurları ve (yazıcının veya diğer dijital cihazların fiziksel teslimi gibi) somut olanları içeren karma işlemler bağlamında da ortaya çıkmaktadır. Bu tür işlemler, NesNet alanındaki ilerlemelerle daha da belirginleşecektir. Sınıflandırma konusu, mallar ve hizmetler için farklı düzenleyici mekanizmalar nedeniyle önemli etkilere sahiptir.

TRIPS ile İnternet üzerinde IPR'nin korunması arasındaki bağlantı ne olmalıdır?

DTÖ'nün TRIPS anlaşması IPR için WIPO anlaşmalarından çok daha güçlü uygulama meka-

nizmaları sağladığından, gelişmiş ülkeler TRIPS kapsamını iki yaklaşımı kullanarak e-ticarete ve İnternete kadar genişletmeye çalışmaktadır. Birincisi, bu ülkeler teknolojik tarafsızlık ilkesine dayanarak, diğer DTÖ kuralları gibi, TRIPS'in İnternet de dahil olmak üzere herhangi bir telekomünikasyon ortamına genişletilmesi gerektiğini savunmaktadır. İkincisi, bazı gelişmiş ülkeler WIPO'nun "dijital anlaşmalarının" TRIPS sistemine daha fazla entegrasyonunu istemektedir. Her iki mesele de kapanmamıştır ve gelecekteki DTÖ müzakerelerinde giderek daha önemli hale gelmesi muhtemeldir. Küresel e-ticaret düzenlemelerinin eksikliği, (sözleşmeler ve imzalar gibi) bazı spesifik girişimler ve başta AB ve Asya Pasifik bölgesinde olmak üzere çeşitli bölgesel anlaşmalarla kısmen telafi edilecektir.

DTÖ'nün e-ticarete gelecekteki rolü

DTÖ'nün e-ticarete artan bir rol oynaması gerekip gerekmediğine dair tartışmalar devam etmektedir. Eylül 2016'da yapılan DTÖ Kamu Forumu sırasında, örgütün e-ticareti ve genel dijital ekonomiyi gündemine daha güçlü bir şekilde dahil edebileceği ileri sürülmüştür.¹³ Ancak, üye ülkeler bu konuda hemfikir görünmemektedir. Bazıları, e-ticarete daha fazla odaklanmaya ve bu alanda çok taraflı çerçeveleri göz önünde bulundurmaya istekli olduğunu gösterirken, diğerleri düzenleyici çerçevelerin tartışılmasından önce DTÖ'nün odaklanması gereken (altyapıya ve dijital becerilere erişim gibi) başka öncelikler olduğu görüşündedir.¹⁴

E-ticaret ve diğer dijital politika meseleleri

E-ticaret ile diğer internet yönetişi sorunları arasında net bir ayırım yapmak giderek daha zorlaşmaktadır. Örneğin, veri ekonomisinin ticari boyutu, kaçınılmaz olarak, gizlilik ve bilgi özgürlüğü (örneğin BMMYK içerisinde ele alınan konular), (ISO, IETF, ITU tarafından geliştirilen) veri işlem standartları, verilerin (UN GGE, UNODC gibi kurumlarca) terör ve suçla karşı mücadelede giderek daha önemli bir rol oynadığı durumlarda siber güvenlik konusundaki insan hakları düzenlemelerinden etkilenir. DTÖ, ticaretin ötesindeki dijital politikanın tüm karmaşıklığı ile uğraşmasa da (ve uğraşmamalı da), kuruluşun e-ticaret konusundaki çalışmalarını, DTÖ'nün e-ticaret düzenlemelerini kaçınılmaz biçimde etkileyecek diğer uluslararası kuruluşların çalışmaları ile senkronize etmek için mekanizmalar geliştirmek zorundadır.

Diğer küresel e-ticaret girişimleri

E-ticaretle ilgili konularla ilgilenen birkaç uluslararası kuruluş vardır. UNCITRAL bu alanda önemli çalışmalar yapmıştır. 1992'de UNCITRAL, diğerleri çalışmalarının yanında, UNCITRAL, çalışmaları [Elektronik Ticaret Yasası Modelinin](#)¹⁵ ve [Uluslararası Sözleşmelerde Elektronik Haberleşmelerin Kullanımı konusundaki Birleşmiş Milletler Konvensiyonun](#)¹⁶ kabul edilmesine yol açan Elektronik Veri Değişimi üzerine bir Çalışma Grubu oluşturmuştur. Model Yasası, alandaki en başarılı ve yaygın olarak desteklenen uluslararası inisiyatiflerden biri olmuştur; e-ticaretin geleneksel ticaret yasasıyla entegrasyonuna yönelik mekanizmalara odaklanmaktadır (örneğin, elektronik belgelerin geçerliliğinin tanınması). Model Yasası, birçok ülkede e-ticaret düzenlemesi için temel olarak kullanılmıştır.

E-ticaret alanında bir başka girişim, BM Ticaret Kolaylaştırma ve Elektronik Ticaret Merkezi (CEFACT) ve Yapısal Bilgi Standartlarının Geliştirilmesi Teşkilatı (OASIS) tarafından başlatılan **Elektronik İşletme XML** (ebXML) Girişimidir. Girişimin amacı, yerli ve uluslararası elektronik ticaret değişimlerini destekleyen ilgili ve açık teknik özellikler geliştirmektir.¹⁷ Yeni özellikler geliştirilirken, önceki set olan Elektronik Veri Değişimi (EDI) hala yaygın olarak kullanılmaktaydı. Mesele bu özelliklerin yeni trendlerle ve teknolojik gelişmelerle başa çıkmak için kullanılıp kullanılmayacakları ve nasıl ve kullanılacaklarına kalmıştır.

UNCTAD, özellikle e-ticaretin kalkınma ile olan ilgisine odaklanarak, araştırma ve kapasite geliştirmede etkindir. Her yıl bilgi ekonomisinin evrimini izler ve yeni teknolojilerin ticaret ve kalkınmadaki rolünü değerlendiren **Bilgi Ekonomisi Raporu**'nu yayınlamıştır.¹⁸ UNCTAD, 2016 yılında, gelişmekte olan ülkelerin e-ticareti kullanma ve yararlanma yeteneklerini geliştirmeyi amaçlayan çok paydaşlı bir girişim olan **eTrade for All Initiative**'i başlatmıştır.¹⁹

OECD'nin faaliyetleri, tüketicinin korunması ve dijital imzalar dahil, e-ticaret ile ilgili çeşitli yönleri kapsamaktadır. E-ticaret konularına katılımı, dört ana konuda yapılandırılmış 1998 **Elektronik Ticaret Eylem Planı** ile başlamıştır: kullanıcılar ve tüketiciler için güven oluşturmak, dijital pazar için temel kuralları oluşturmak, elektronik ticaret için bilgi altyapısını geliştirmek ve onun faydalarını en üst seviyeye çıkarmak.²⁰ Bu tür konular OECD'nin önerileri ve kılavuzlarında ele alınmıştır.

G20 ayrıca son yıllarda e-ticaretle ilgili konulara daha fazla önem vermektedir. Çin'in Hangzhou kentindeki G20 Liderleri Zirvesi'nde (Eylül 2016), e-ticaret konusunda işbirliği G20 üyelerinin önceliklerinden biri olarak vurgulanmıştır.²¹ Liderler ayrıca, temel olarak küçük ve orta ölçekli işletmelerin (KOBİ'lerin) küresel e-ticaret piyasasına katılmaları için yardım etmeyi amaçlayan bir **Elektronik Dünya Ticaret Platformu** oluşturma girişimini not etmişlerdir.

İş sektöründe, en aktif uluslararası organizasyonlardan biri, e-ticaret alanında geniş kapsamlı tavsiyeler ve analizler üreten Uluslararası Ticaret Odası'dır (ICC).

Bahsetmeye değer bir diğer girişim BM Küresel İlkeler Sözleşmesidir. Özellikle e-ticaretle ilgili meseleleri ele almayı amaçlamamasına rağmen, girişim, işletmeler ve insan hakları arasında daha güçlü bağlantılar kurmaya ve şirketlerin sorumluluklarını insan hakları konusundaki evrensel ilkelerle uyumlu hale getirerek şirketleri sorumlu bir şekilde iş yapmalarını desteklemeye yöneliktir. Dijital ortamda insan haklarının korunmasına ilişkin hususlar, İnternet şirketlerinin işlerini yürütme şeklini giderek daha fazla etkilediği için, bu girişimin, e-ticaret alanında da dahil olmak üzere İnternet endüstrisi üzerinde önemli bir etkisi olması beklenmektedir.

Bölgesel girişimler

AB, ilk e-ticaret stratejisini Lizbon'daki AB liderlerinin Dot Com Zirvesi olarak anılan toplantıda (Mart 2000) geliştirmiştir. E-ticarete özel ve pazar merkezli bir yaklaşımı benimsemesine rağmen, AB (evrensel erişimin teşvik edilmesi, halkın çıkarlarının dikkate alınmasını içeren bir rekabet politikası ve zararlı içeriğin dağıtımında bir kısıtlama gibi) ayrıca kamu ve sosyal çıkarları korumayı amaçlayan bir kaç önlem almıştır. Daha sonra, 2015 yılında **Dijital Tek**

Pazar Stratejisi kabul edilmiştir. Bu belge Dijital ürünlere ve hizmetlere çevrimiçi erişimi kolaylaştırmak ve dijital ekonomiyi büyümenin itici gücü olarak güçlendirmek hedefleriyle e-ticarete güçlü bir şekilde odaklanmıştır.

AB ayrıca (bir AB üye ülkeleri arasında elektronik ticaret için tek tip ve kapsamlı bir yasal çerçeve getirmeyi) ve elektronik imzalar, veri koruma ve elektronik finans ile ilgili diğer yasal araçları devreye sokmayı amaçlayan **E-ticaret Yönergesi** çıkarmıştır.

Asya Pasifik bölgesinde, e-ticaret işbirliğinin odak noktası APEC'dir. APEC'in e-ticaretle ilgili ilk programlardan biri, bu alandaki çeşitli APEC girişimlerini pekiştirmeyi ve uygulamayı amaçlayan 1998 **APEC Elektronik Ticaret Eylem Planı**'dır. Bu planı uygulamak için, tüketicinin korunması, veri koruması, spam ve siber güvenlik dahil olmak üzere çeşitli e-ticaret sorunlarını ele almak üzere bir E-Ticaret Yönlendirme Grubu kurulmuştur. En belirgin girişim, sınır ötesi ticarete kağıtsız sistemler oluşturmayı hedefleyen APEC'in **Kağıtsız Ticaret Bireysel Eylem Planı**'dır.²²

ASEAN bünyesinde, tüketiciler için güven ve güven yaratan e-ticaret düzenleyici ve yasal çerçevelerin geliştirilmesine katkıda bulunmak amacıyla E-ticaret ve BİT Ticaret Kolaylıkları Çalışma Grubu kurulmuştur. Bu bağlamda, grup, bir e-ticaret yasal altyapısı için kılavuzlar oluşturmayı ve ASEAN ülkeleri içinde ve arasında güvenilir e-ticaret ve e-ticaretin gelişmesini ve büyümesini kolaylaştırmayı amaçlayan E-ticaret Yasal Altyapı Projesini başlatmıştır.

Doğu ve Güney Afrika Ortak Pazarı (COMESA) da e-ticaret alanında çalışmalar yürütmektedir. COMESA Stratejisi, kuruluşun ortak pazarın dijital entegrasyonunu geliştirmek için e-ticareti aktif olarak destekleme konusundaki taahhüdünü ana hatlarıyla belirtmektedir. 2010 yılında, COMESA Konseyi, elektronik imzalar, e-ticaret, tüketicinin korunması, istenmeyen ticari iletişim ve çevrimiçi uyuşmazlık çözümüne ilişkin hükümler içeren bir **Elektronik İşlemler Modeli Yasasını** kabul etmiştir.²³

Çok taraflı girişimler

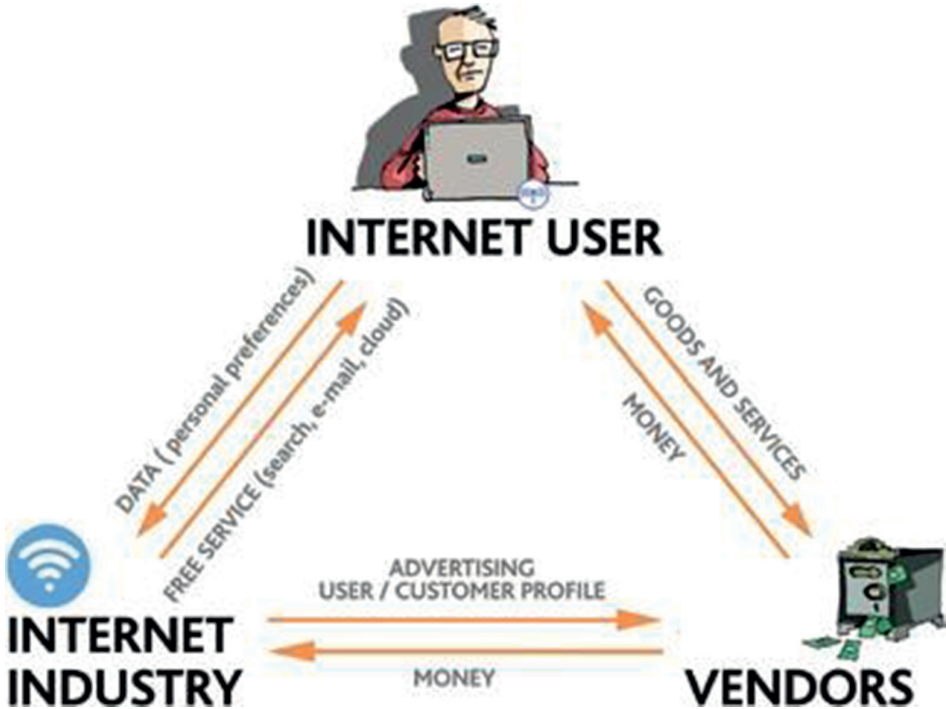
Çok taraflı girişimler, aynı konularla ilgilenen farklı bölgelerden ülkeleri bir araya getirmektedir. Çok taraflı yaklaşım DTÖ bağlamında giderek daha fazla kullanılmaktadır. Son zamanlarda birkaç bölgesel bölgesel ticaret anlaşması müzakere edilmiştir ve bunların dijital politika üzerinde önemli bir etkisi olması beklenmektedir. En göze çarpan anlaşmalardan ikisi Şubat 2016'da imzalanan **Trans-Pasifik Ortaklığı** (TPP) ve Ekim 2016 itibarıyla halen görüşülmekte olan **Transatlantik Ticaret ve Yatırım Ortaklığı**'dır (TTIP). Bu ticaret anlaşmaları sadece e-ticareti etkilemeyecek, aynı zamanda internet konularında veri düzenleme ve anlaşmazlıkların çözümü etkileyecektir.

www.igbook.info/ecommerce

İnternet VERİ ekonomisi

İnternet endüstrisinin ağırlıklı olarak Silikon Vadisi merkezli şirketler tarafından geliştirilen yeni iş modeli (Şekil 19) 1990'ların sonunda ortaya çıkmaya başlamış ve 2010'larda tam olarak şekillenmiştir. İnternetin 1990'larda büyümesi, geçmişte olduğu gibi kamu kaynakları üzerinden sürdürülemedi; çünkü daha sağlam bir iş modeli gerektiriyordu. İnternet servislerine ve içeriğe erişim için birkaç deneme girişiminde bulunulmuştur. Yeni İnternet işletme modeli, kullanıcıları İnternet servislerinin kullanımı için ücretlendirmemekte; bunun yerine sofistike reklamcılıktan gelir elde etmektedir.

Bu yeni iş modelinde, kullanıcı verileri temel ekonomik kaynaktır. Bilgi ararken ve İnternet üzerinde etkileşimde bulunurken, kullanıcılar kişisel veriler ve ürettikleri bilgiler de dahil olmak üzere 'elektronik ayak izi' olarak bilinen önemli miktarlarda veri dağıtırlar. İnternet şirketleri, kullanıcı tercihleri, zevkleri ve alışkanlıkları hakkında bilgi parçaları çıkarmak için bu verileri toplar ve analiz eder. Ayrıca bir grupla ilgili bilgileri çıkarmak için veriyi kullanırlar; örneğin, gençlerin belirli bir şehir veya bölgedeki davranışları gibi. İnternet şirketleri, belirli bir profili olan bir kişinin ne alacağını ya da ne yapacağını kesin olarak tahmin edebilirler. İnternet kullanıcıları hakkındaki bu değerli veri bloğunun farklı ticari kullanımları vardır, ancak temel olarak pazarlama faaliyetleri için kullanan satıcılara hizmet eder.



Şekil 19. İnternet işletme modeli

Meseleler

Kullanıcıların korunması ve şeffaflık

Doğrusunu söylemek gerekirse, kullanıcılar genellikle uzun ve ayrıntılı sözleşme hükümlerini ‘Kabul ediyorum’ butonuna tıklayarak servis sağlayıcı tarafından belirlenen koşulları kabul ederler. Kullanıcıların, özellikle verilerinin ticari amaçlarla kullanma potansiyeli açısından, bilinçli kararlar alıp almadıklarına dair soru ortada durmaktadır. Büyük olasılıkla, çoğu durumda, kullanıcıların, değerli İnternet hizmetleri karşılığında verilerini değişmeyi ciddi şekilde düşünmeden kabul etmektedirler. İnternet düzenlemelerinin daha şeffaf ve anlaşılması kolay olması sadece kullanıcılar için değil, aynı zamanda, İnternet kullanıcılarının bilinçli tercihlerine dayanarak daha sürdürülebilir bir iş modeli sağlayabilen İnternet şirketleri için de daha faydalıdır.

Hakim piyasa pozisyonlarının kötüye kullanılması riski

İnternet endüstrisi, piyasa tekellerinin kurulmasına yatkındır. Örnek olarak, Ağustos 2016’da Google’ın arama motoru pazarındaki payı masaüstü aramalarında % 70, mobil/tablet aramalarında ise % 90’dan fazla olmuştur.²⁴

Şirketler tekel (veya baskın) piyasa pozisyonlarına sahip olduğunda, bazen bu tür pozisyonları kötüye kullanma ve yeni şirketlerin pazara girmelerini engelleyen veya zorlaştıran engeller ortaya koyma eğilimindedir. Bu tür meseleleri ele almak için, ilgili ulusal ve/veya bölgesel yetkililerin etkili ve etkin izleme mekanizmalarının yanı sıra yeterli rekabet ve antitröst politikaları ve mevzuatını geliştirme ve uygulama yeteneğine sahip olmaları gerekir. Her ne kadar bu politikalar ve yasalar ülkeye veya bölgeye özgü olsa da, yerel veya bölgesel düzeyde faaliyet gösteren küresel İnternet şirketlerinin rekabet karşıtı davranışlarını etkin bir şekilde ele almak için kullanılabilir. Örneğin, AB, bu alandaki gelişmiş piyasa düzenlemeleri nedeniyle, yasadışı uygulamaların önlenmesi veya ele alınması ve İnternet şirketlerinin düzenlemeleri izlemeye zorlaması için birçok girişimde bulunmuştur. Son yıllarda, Avrupa Komisyonu, AB dijital pazarındaki rekabeti izleme konusunda oldukça aktif hale gelmiştir. Bunun bir sonucu olarak, Avrupa Komisyonu baskın piyasa pozisyonlarını kötüye kullandığı söylenen internet şirketlerine karşı bazı girişimlerde bulunmuştur. Google, diğerlerinin yanı sıra şirketin reklamcılıkla ilgili uygulamalarına odaklanan bu girişimlerin bazılarının hedefi olmuştur.

İnternet ERIŞİM ekonomisi

İnternet kullanıcıları ve internet şirketleri internet erişimi ile ilgili hizmetler için ISS’lere ödeme yapar. Genellikle, ISS’ler, toplanan ücretlerden aşağıdaki masrafları karşılamak zorundadır:

- Telekomünikasyon giderlerinin ve bir sonraki ana İnternet hub’ına bağlanan internet bant genişliğinin maliyeti.
- RIR’lerden veya yerel LIR’lerden elde edilen IP adreslerinin maliyeti. İnternete giren her cihazın bir IP adresine ihtiyacı vardır.
- Ekipman ve yazılım edinme, kurma ve bakım maliyeti (Şekil 20).

Avrupa, bir telekomünikasyon operatörü ETNO aracılığıyla, Dubai'deki WCIT-12 hazırlıkları sırasında, (Facebook, Google gibi) içerik sağlayıcılarının kendi hizmetlerine erişim için ödeme yapmalarını önerdiklerinde bu tartışmalara yol açmıştır. Teklif o zaman destek almadı, ancak gelecekteki İnternet yönetişimi müzakerelerinde açık bir sorun olarak ortada duracağı benzenmektedir.

İnternet gelirinin yeniden dağıtımı hakkındaki bu tartışma, ağ tarafsızlığı tartışmasını güçlü bir şekilde desteklemektedir. Örneğin, tüm İnternet trafiğine eşit muamele edilmeli mi, yoksa (VIP İnternette yoksullar için bir internette seçeneklerin listesi gibi) hizmetlerin kalitesine, ödemeye ve güvenilirliğe bağlı olarak farklı kademelere ayrılmalı mı?

Paket başına ödemeye karşılık sabit oran

İnternetteki sabit oranlar üzerine yapılan tartışma genellikle üç unsur arasında uygun ve optimal bir dengeye oturtulması ile çerçeveslenmektedir: teknik verimlilik, ekonomik verimlilik ve sosyal etkiler.²⁵ Bazı yazarlar mevcut, basit, sabit oranlı fiyatlandırma yapısını, paketlerin trafiğine dayanan muhasebe gibi daha karmaşık olanlarla değiştirmenin zorluklarını vurgulamaktadır.²⁶ Pratik değişikliklerle ilgili olarak, bazıları mevcut İnternet fiyat politikalarını değiştirmenin, çözümlerden daha çok sorunları tetikleyerek bir Pandora'nın kutusunu açabileceğine inanmaktadır.

Telekomünikasyon gelirini geliştirmekte olan ülkelerle paylaşmak

Gelişmekte olan birçok ülke, İnternet ekonomisinin ekonomik koşullarının eşitliği hakkında sorular ortaya atmaktadır. Her uluslararası çağrının ücretinin iki ülke arasında paylaşıldığı geleneksel telefon sistemine kıyasla, İnternet modeli tüm yükü bir tarafa koyuyor: gelişmekte olan ülkelere gelen kullanıcılar, çoğunlukla gelişmiş ülkelere bulunan İnternet omurgalarına bağlantıyı finanse etmek zorunda kalabilmektedir. Sonuçta, paradoksal olarak, küçük ve fakir ülkeler, gelişmiş ülkelere interneti sübvansede bilmektedir.

Finansal uzlaşma sorunu, önemli bir bütçe kaynağı olarak uluslararası telekomünikasyonlardan elde edilen gelire dayanan en fakir ülkeler için özellikle önemlidir. VoIP'nin internet telefonunu ortaya çıkarmasıyla telefon trafiğini ulusal telekomünikasyon operatörlerinden internete kaydırması ile durum daha da karmaşık hale gelmiştir.

Gelişmekte olan ülkeler, WSIS sırasında, ITU çalışma gruplarında ve WCIT-12'de, birden fazla bağlamda daha adil İnternet erişimi iş modelleri sorununu gündeme getirmiştir.

Ortaya çıkan trendler: Nesnelerin İnterneti, yapay zeka, ekonomi paylaşımı

NesNet, İnternet ekonomisi üzerinde büyük bir etkisi olan yükselen bir eğilimdir. NesNet'nin iş modellerine entegrasyonu maliyetleri düşürür ve verimliliği artırır. Pek çok yeni işletme şimdi enerji maliyetlerini optimize etmek ve çevreyi korumak için "akıllı binalar" kullanmaktadır. BİT çözümlerinin iş süreçlerine uygulanması, işletmelere geleneksel çevrelerden daha hızlı bir

şekilde gelişmelerine yardımcı olan rekabet avantajı sağlamaktadır. İşletmeler bu nedenle, genel ekonomik refahı önemli ölçüde artıran BT endüstrisinden yeni, özel ve yenilikçi yaklaşımlar talep etmektedir.

AI alanındaki ilerlemelerin de önemli ekonomik etkilere sahip olması beklenmektedir. Bir tarafta, AI tarafından getirilen yeni otomasyon dalgasının önemli ölçüde verimlilik artışı sağlaması olasıdır. Öte yandan, bu otomasyonun işler ve istihdam üzerindeki etkisine ilişkin endişeler dile getirilmektedir.

İnternet ekonomisindeki en son model, Uber ve Airbnb gibi yeni oyuncular küresel pazara tanıtan sözde **paylaşım ekonomisi**dir. Bu tür işletmeler, dijital çözümleri iş süreçlerine entegre ederek, böylece işletme maliyetlerini düşürerek ve tüketicilere daha doğrudan erişerek İnternet ekonomisi tarafından sunulan fırsatlardan tam olarak faydalanmışlardır. Aynı zamanda, bu tür modeller taksi ve otel hizmetleri gibi geleneksel işletmelerden tepki almışlardır. Paylaşım ekonomisi için (sorumluluk, tüketicinin korunması, vergilendirme gibi) özel düzenlemelere ihtiyaç duyulup duyulmadığına ve hatta hükümetlerin bu kategoriye giren hizmetleri yasaklamasının gerekip gerekmediğine dair tartışmalar devam etmektedir. AB, şimdilik, “bekle ve gör” yaklaşımını seçmiştir. Avrupa Komisyonu, Haziran 2016’da, **işbirlikçi ekonomi için bir Avrupa Gündemi** ile ilgili üye devletlere, mevcut AB mevzuatının işbirlikçi ekonomiye ne şekilde uygulanması gerektiği konusunda rehberlik sağlamayı amaçlayan bir tebliğ yayımlamıştır. Komisyon ayrıca, paylaşım ekonomisine mutlak yasaklar getirmenin yalnızca son çare tedbiri olduğunu ileri sürmüştür.²⁷

E-ticaretin bir yan ürünü ortaya çıkan **bağımsız piyasadır**. Bir yandan bu, bağımsız çalışan enerjik bir iş topluluğunun yükselmesine neden olmuş ve KOBİ’lerin güçlendirilmesine ve işsizliğin azaltılmasına katkıda bulunmuştur. Öte yandan, yalnızca çevrimiçi bağımsız çalışmanın getirdiği gelir muamelesinden dolayı olmasa da, emeğe yeni bir yaklaşım gerektirmektedir.

İnternet ekonomisine önemli ölçüde katkıda bulunan bir diğer alan ve aynı zamanda çok sayıda tartışmayı gündeme getiren **e-kumardır**. Eşsiz özelliklerinden dolayı e-kumar oynamaya farklı düzenleyici yaklaşımlar uygulanmıştır. Örneğin, AB düzenlemeyi üye devletlere bırakmaktadır. Bu alanın duyarlılığı ve kamu politikaları, ahlak, küçüklerin korunması ve siber güvenlik suçları ile ilişkisi, e-kumar düzenlemesinin, her ülkenin politik ve sosyal geçmişine göre ulusal düzeyde gerçekleştirilmeye daha uygun olduğu iddia edilmiştir.

www.igbook.info/othereconomic

E-bankacılık, e-para ve sanal para

Dijital nakit, gezegende kendi para birimini yönetmek isteyen her hükümet için bir tehdittir.

David Saxton, Net’in kurucusu.²⁸

E-bankacılık

E-bankacılık, kart ödemeleri veya fon transferleri gibi geleneksel bankacılık işlemlerini yürütmek için İnternet'in kullanılmasını içerir. Yenilik sadece aracıdadır; bankacılık hizmeti temelde aynı kalır. E - bankacılık, çevrimiçi erişim ve kağıtsız seçeneklerden yararlanarak ve işlem maliyetlerini azaltarak müşterilere avantajlar sağlar. Örneğin, geleneksel bankacılıkta 4 ABD Doları olan müşteri işlemlerinin e - bankacılık'ta yalnızca 0,17 ABD Doları olduğu tahmin edilmektedir.²⁹

E-para

Elektronik para ya da e-para, elektronik olarak tutulan bir karta veya uzaktan bir sunucuya kaydedilen para bakiyesidir. Uluslararası Takas Bankası (BIS), e-parayı 'satış noktası terminaleri üzerinden, iki cihaz arasında doğrudan transferler veya İnternet gibi açık bilgisayar ağları üzerinden yapılan ödemeler için saklanan değer veya ön ödemeli ödeme mekanizmaları olarak' tanımlamaktadır.³⁰ E-para mevcut bankacılık ve para (ulusal bankalar tarafından denetlenen kâruni para) sistemine bağlanır. Genellikle Mondex ve Visa Cash gibi şirketler tarafından verilen akıllı kartlarla ilişkilendirilir.

Dijital para birimi, sanal para birimi ve kripto para birimi

Değeri değişmeden kalan (EUR ve USD gibi) resmi para birimini temsil eden geleneksel e-paranın aksine, **dijital para** herhangi resmi para birimine eşdeğer değildir (ve ulusal finans sisteminin bir parçası değildir ve bu nedenle devlet yetkilileri tarafından düzenlenmez).

Dijital para birimleri ya merkezi olabilir ya da merkezi olmayabilir. Merkezi bir modelde, para biriminin düzenlenmesi ve para biriminin kullanımı ve dolaşımına ilişkin kuralları uygulama ve yürütme mekanizmaları, merkezi bir tarafça yönetilir. Merkezi olmayan bir modelde, bu tür işlemler ağdaki çeşitli taraflarca yönetilir.

Hem **sanal para** birimleri hem de **kripto para** birimleri, dijital para birimleridir. Sanal para birimleri merkezi bir modele dayanırken, (güvenlik için kriptografi kullanan ve bu yüzden sahte olması zorlaşan dijital para birimleri olan) kripto para birimleri ya merkezi olabilir ya da merkezi olmayan bir hale getirilebilir. Bitcoin, merkezi olmayan kripto para biriminin bir örneğidir.³¹

Avrupa Merkez Bankası, 2012 yılında (sanal para birimleri olan) sanal parayı "geliştiricileri tarafından verilen ve genellikle kontrol edilen ve belirli bir sanal topluluğun üyeleri arasında kullanılan ve kabul edilen" bir tür düzenlemesiz, dijital para olarak tanımlamıştır.³² 2014 yılında, Avrupa Bankacılık Otoritesi, sanal para birimini "bir merkez bankası veya kamu otoritesi tarafından verilmeyen ya da zorunlu olarak resmi bir para birimine bağlı olmayan, ancak gerçek ya da tüzel kişiler tarafından transfer edilebilir, saklanabilir veya ticareti yapılabilir ödeme aracı olarak kabul edilen bir dijital para gösterimi" olarak tanımlamıştır.³³

Kripto para birimleri, popüleriteleri ve kullanımları arttıkça, çevrimiçi dünyayı rüzgarına kaptırmaya hazırlar. Apple, Dell ve PayPal gibi büyük şirketler kripto para birimlerini bir ödeme

yöntemi olarak entegre etme planlarını çoktan belirttiler ve daha fazlasının takip etmesi de muhtemeldir.

Son yıllarda, Bitcoin en popüler kripto para birimlerinden biri olarak ortaya çıkmıştır ve Bitcoin kullanımına izin veren hizmetlerin sayısı büyük ölçüde artmıştır.

Bitcoin

Bitcoin kullanımı blockchain teknolojisine dayanmaktadır, bu da tüm işlemlerin bir bilgisayar ağında paylaşılan dağıtılmış bir veritabanı (P2P ağı) olan merkezi bir defteri olduğu anlamına gelir. Bu açık kaynaklı yazılım, bir ağdaki tüm akranların Bitcoin’de yapılan tüm işlemleri doğrulamasını sağlar ve bu nedenle bu merkezi defterin koruyucusu olarak hizmet eder. Düğümler (ağlardaki akranlar bilindiği gibi) işbirliği içinde çalışırlar, aralarında çok az etkileşim vardır ya da hiç olmaz, karşılıklı doğrulamayı işlem kromatolojisinin kanıtı olarak kabul ederler. Bu “defter”, dürüst düğümlerin tüm işlem (işlemci) gücü dürüst olmayan düğümlerden daha yüksek olduğu sürece güvenlidir.

Üretilen bitcoin sayısı 21 milyon ile sınırlıdır, yani dijital para biriminin değeri zamanla artar (erken sahip olanlar ödüllendirilir). Herkes daha önce çözülmemiş matematiksel hesaplamalı bir problemin çözümünü ileterek (iş sisteminin kanıtını kullanarak) Bitcoin (‘madeni’) oluşturabilir. Tüm düğümler bu “sorun” üzerinde çalışır ve çözüm bulunduğunda, bu blok kapatılır ve tüm düğümler (bu zincirdeki bir sonraki blok olan) bir sonraki soruna ilerler. Düğümler veya adlandırılan “madenciler”, bilgisayarlarının gücünü ağ güvenliğine adadıkları için ödüllendirilirler. Bu ödül belirli sayıda bitcoin ve başkaları tarafından ödenen işlem ücretlerini içerir.

Kripto para birimlerinin temel avantajları, geleneksel bankacılık sistemine kıyasla düşük ücretler, hızlı ve şeffaf ödemeler ve mobil erişimdir. Bu avantajlar, başlangıç faaliyetlerini artırabilir ve gelişmekte olan ülkelerin, küresel pazarda gelişmiş ülkelerle eşit düzeyde ayakta durmalarına yardımcı olabilir.

Artık dünya çapında pek çok hizmet Bitcoin’i ödeme aracı olarak kabul ediyor ve bu tür işlemler bazı ülkelerde katma değer vergisinden (KDV) muaf tutuluyor. Temmuz 2015’te CJEU, Bitcoin’in geleneksel para birimleri ile çevrimiçi değişiminin, tıpkı banknot ve madeni para işlemlerinde olduğu gibi, tüketim vergisinden muaf tutulması gerektiğine karar verdi.

Merkez bankalarının sanal para birimlerine gittikçe daha fazla dikkatlerini yoğunlaştırdıklarına dair işaretler de bulunmaktadır. Örnek olarak, 2016’nın başlarında, Çin Halk Bankası, bunun kara para aklama ve vergi kaçakçılığını azaltacağını, ekonomik faaliyetlerin daha şeffaf olmasına katkıda bulunacağını göz önünde bulundurarak kendi sanal para birimini başlatma olasılığını araştırdığını açıkladı.³⁴

2016 yılında, Uluslararası Para Fonu (IMF), [Sanal Para Birimleri ve Ötesi: İlk Değerlendirmeler](#) raporunu yayınladı. Raporda, tüketicinin korunması, vergilendirilmesi ve finansal istikrar dahil olmak üzere sanal para birimlerinin düzenlenmesi ve politikaları ile ilgili farklı zorluklar olduğu belirtiliyor. Rapora göre, uygun politikanın ‘düzenlemeyi, inovasyona boğmadan riskleri uygun bir şekilde ele almaya ihtiyaç duyacağı yönündedir’. Uluslararası düzeyde, en iyi uygulamalar ve uluslararası standartlar düzenleyici önlemleri yönlendirmeli ve yargıda uyumu desteklemelidir.³⁵

Meseleler

Dünya çapında bankacılık sistemindeki değişiklikler

Hem e-bankacılığın hem de e-paranın daha fazla kullanılması, dünyadaki bankacılık sistemindeki değişiklikleri beraberinde getirerek müşterilere ek olanaklar sağlarken, aynı zamanda bankacılık ücretlerini de azaltabilir. Tuğla ve harç bankacılığı yöntemleri, daha uygun maliyetli e-bankacılık ile ciddi şekilde zorlanacaktır. Geleneksel bankaların çoğunun zaten e-bankacılığını benimsemiş olduğu belirtilmelidir. 2002’de ABD’de çevrimiçi hizmetler sunan sadece 30 banka vardı. Bugün e-bankacılık hizmetleri olmayan bir banka bulmak zordur.

Mobil ticaret

Teknoloji ve cihazlar geliştikçe ve geliştikçe, e-ödemeler ve e-para şu anda hızlı bir değişim geçiriyor. Mobil ödemeler, mobil telefonlar daha sofistike hale geldiğinden ve mobil ticaret de dahil olmak üzere çeşitli uygulamalara olanak tanıyan (akıllı telefonlar ve iPhone’lar gibi) ‘akıllı teknoloji’ sayesinde SMS yoluyla verilen basit siparişleri çoktan aşmıştır.

Siber güvenlik

Siber güvenlik, e-ödemelerinin yaygınlaştırılmasının önündeki en büyük zorluklardan biridir. İnternet üzerinden finansal işlemlerin güvenliği nasıl sağlanabilir? Çevrimiçi işlemlerin güvenliği için bankaların ve diğer finansal kuruluşların sorumluluğunu vurgulamak önemlidir. Bu bağlamdaki ana gelişme, ABD Kongresi tarafından Enron, Arthur Andersen ve WorldCom finansal skandallarına tepki olarak kabul edilen **Sarbanes-Oxley Yasası (SOXA)**³⁶ idi. Bu yasa, finansal kontrolü sıkılaştırmış ve finansal kurumların çevrimiçi işlemlerin güvenliği konusundaki sorumluluğunu artırmıştır. Ayrıca, güvenlik sorumluluğu yükünü de belirli bir ihtiyat göstermesi gereken müşteriler ile finansal kurumlar arasındaki paylaştırmıştır.

E - ödeme yöntemlerinin mevcut olmayışı

E-ödeme yöntemlerinin mevcut olmayışı, genellikle e-ticaretinin daha hızlı gelişmesinin önündeki en temel engellerden biri olarak görülmektedir. Şu anda, e-ticaret öncelikle kredi kartı ile yapılmaktadır. Bu, gelişmiş bir kredi kartı pazarına sahip olmayan gelişmekte olan ülkeler için önemli bir engeldir. Bu ülkelerdeki hükümetlerin, kart ödemelerinin daha hızlı yapılmasını sağlamak için gerekli yasal değişiklikleri kabul etmesi gerekecektir.

Ulusal ve bölgesel girişimler

E-ticaretin gelişimini teşvik etmek için dünya çapında hükümetlerin, kredi kartları ve e-para dahil olmak üzere tüm nakit içermeyen ödemeleri teşvik etmesi gerekir. E-para’nın daha hızlı tanıtılması ek hükümet düzenleme faaliyetleri gerektirecektir.

İlk e-para yasasını çıkartan Hong Kong’dan sonra, AB 2000 yılında (2009’da revize edilen) **Elektronik Para Direktifini** kabul etmiştir.³⁷ E-paradan farklı olarak, AB’de henüz dijital ve/veya sanal para biriminin düzenlenmesi yoktur. Halihazırda Bitcoin gibi para birimlerini düzenleme

işi üye devletlere bırakılmıştır. Almanya, Bitcoin'i iki kişi veya kurum arasında alınıp verilen "özel para" olarak değerlendirmektedir. İngiltere'de, bu bir değişim aracı olarak kabul edilir, ancak para değildir. Çoğu ülke "bekle ve gör" yaklaşımını seçmiştir. Rusya ve Tayland gibi diğer ülkeler, Bitcoin işlemlerini ulusal düzeyde yasaklama konusunda daha radikal adımlar atmıştır.

Uluslararası girişimler

İnternetin doğası gereği, e-para ve sanal para birimlerinin küresel bir fenomen haline gelmesi olasıdır, bu nedenle bu konuyu uluslararası düzeyde ele almak için bir neden ortaya çıkmıştır. E-bankacılık alanında potansiyel bir oyuncu, **Basel Komitesi E-Bankacılık Grubu**'dur. Bu grup, e-para girişinde kilit öneme sahip olan yetkilendirme, ihtiyati standartlar, şeffaflık, mahremiyet, kara para aklama ve sınır ötesi denetim konularını ele almaya başlamıştır.³⁸

Sanal para birimi ile ilgili ana uluslararası girişim, kara para aklama ve terörizmin finanse edilmesi ile ilgili soruları ele alan **Mali Eylem Görev Gücü**'nde (FATF) gerçekleştirilmiştir. ABD, FATF'de kara para aklama konusunda kuralların nasıl uygulanacağı ve terörün finansmanı konusunda sanal para birimleri üzerinde tartışmalar başlatmıştır.

Yasayı uygulayan kolluk kuvveti

2002 New York Eyalet Başsavcısı'ndan PayPal'a ve Citibank'tan Internet kumarhanelerine ödeme yapmama isteği, kolluk kuvvetlerinin görevlerini yerine getirmek için e-ödeme sistemlerini kullanmaya nasıl başladıklarına bir örnektir.³⁹ Kanun uygulayıcı yasal mekanizmalar aracılığıyla yapılamayan elektronik ödemelerin kontrolü ile başarılmıştır.

Mahremiyet

Her e-ödeme işlemi, e-ödeme aracının düzenleyicileri (kredi kartı şirketleri, bankalar) tarafından kaydedilen bir iz bırakır. Bu tür kayıtların tutulması, temiz için ve ödemelerin kanıtı olarak gerekmele birlikte, bu tür verilerin toplanması, veri madenciliği bunları izleme ve harcama alışkanlıklarını izlemek veya müşterileri sonraki mali hizmetler için puanlamak maksadıyla kullanılıyorsa, kullanıcıların gizliliği için ciddi tehditler oluşturabilir.

Sanal para birimlerinin riskleri ve kötüye kullanımı

En büyük Bitcoin çevrimiçi döviz piyasalarından biri olan Mt Gox'un Şubat 2014'te kapatılmasının ardından sanal para biriminin riskleri belirginleşti.⁴⁰ Çok sayıda yatırımcı, kullanıcı hesabı hırsızlığı ile 500 milyon ABD dolarına yakın bir değer kaybetmiştir.

Sanal para birimlerinin yasadışı mal ve hizmetler, dolandırıcılık ve kara para aklama için potansiyel olarak kötüye kullanılabileceği konusunda birçok uyarı vardır. Kriptografik Bitcoin işlemlerinin anonimliği olası yanlış kullanım potansiyelini artırır. Ayrıca, Bitcoin cüzdanları (bitcoin'lerin çevrimdışı olarak depolanabileceği yer) şifrelenebilir.

FBI, 2014 yılında, çalınan kart verilerini, uyuşturucuları ve diğer yasa dışı ürünleri ticaretinde kullanılan Silk Road web sitesini kapatmıştır. Web sitesi ödeme yöntemi olarak Bitcoin'i kullanmıştır.⁴¹

ABD hükümeti tarafından 2015 sonunda yayınlanan ve **Ulusal Para Birimlerinin Ulusal Güvenlik Etkileri** hakkında finanse edilen bir raporda, terör ve hakaret içeren gruplar da dahil olmak üzere “devlet dışı aktörler” in, normal ekonomik işlemler için kullanarak sanal paradan yararlanabileceği belirtmiştir.⁴²

AB, bu tür sorunları yasal tedbirlerle ele almaya çalışmaktadır. Temmuz 2016'da Avrupa Komisyonu, **kara para aklama veya terör finansmanı amacıyla finansal sistemin kullanılmasının önlenmesine ilişkin Direktifi** değiştirme önerisini yayımlamıştır. Teklif, diğerleri arasında Yönerge kapsamına giren sanal para değişim platformlarını şüpheli sanal para işlemlerinin tespiti için yardımcı olacak kontrol önlemlerini almalarını istemiştir. Teklif aynı zamanda sanal para birimleri için yasal bir tanım getirmeyi hedeflemiş ve bu amaçla, Avrupa Bankacılığı Otoritesi tarafından 2014 yılında sağlanan tanıma kullanmıştır.⁴³

www.igbook.info/emoney

Tüketicinin korunması

Tüketici güveni, e-ticaretin başarısının ön koşullarından biridir. E - ticaret hala nispeten yenidir ve tüketiciler gerçek alışverişlerde olduğu kadar güvende değildir. Tüketici koruması, e-ticarete duyulan güveni geliştirmek için önemli bir yasal yöntemdir. E-ticaret düzenlemesi, müşterileri aşağıdaki gibi çeşitli alanlarda korumalıdır:

- Ödeme kartı bilgilerinin çevrimiçi olarak alınması.
- Yanıltıcı reklamcılık.
- Kusurlu ürün teslimi.

E-ticaretin yeni ve spesifik bir özelliği, geleneksel ticarete hayati bir sorun olmayan tüketici korumanın uluslararasılaşmasıdır. Geçmişte, tüketiciler nadiren uluslararası korumaya ihtiyaç duyuyorlardı. Yerel olarak satın alıyorlardı ve bu nedenle yerel müşteri koruması gerekiyordu. E-ticaret ile uluslararası sınırlar arasında artan sayıda işlem gerçekleşmektedir.

Yargı yetkisi, tüketicinin korunmasını çevreleyen önemli bir konudur. İki ana yaklaşımı içerir. Birincisi, (çoğunlukla e-işletme olan) satıcıyı tercih eder ve orijinal menşei veya ülkesi ile satıcı yaklaşımıdır. Bu senaryoda, e-ticaret şirketleri tahmin edilebilir ve iyi bilinen kendi yasal çevrelerine güvenme avantajına sahiptir. Müşteriyi tercih eden bir diğer yaklaşım ise, hedef ülke yaklaşımıdır.

E-ticaret şirketleri için en büyük dezavantaj, çok çeşitli yasal yargı alanlarına maruz kalma potansiyelidir. Bu ikilemin olası bir çözümü, yargı meselesini daha az indirgeyerek, tüketici koruma kurallarının daha iyi bir şekilde uyumlaştırılmasıdır. Diğer e-ticaret konularında olduğu gibi, OECD, 1999 **E-ticaret Bağlamında Tüketici Koruması Kılavuzunu**⁴⁴ ve 2003 **Tüketicileri Sınırlar Arasında Sahte ve Aldatıcı Ticari Uygulamalardan Koruma Kılavuzlarını**⁴⁵ kabul ederek

öncülüğü üstlenmiştir. OECD tarafından oluşturulan ana ilkeler hala geçerlidir ve ICC de dahil olmak üzere diğer iş birlikleri tarafından kabul edilmiştir.

AB, yüksek düzeyde bir e-ticaret tüketicisi koruması sunmuş ve çevrimiçi alışveriş konularında farkındalık kampanyaları başlatmıştır. Yargı yetkisi sorunu, tüketicilerin her zaman yerel yasal korumaya başvurmalarını öngören **Brüksel I Yönetmeliği**⁴⁶ ile ele alınmıştır. Ocak 2015'ten itibaren geçerli olan Brüksel I Tüzüğü,⁴⁷ AB'de ikamet etmeyen bireylerin AB üye devletlerinin mahkemelerinde tüketiciler tarafından dava edilebileceği durumları artırarak yargı kurallarını daha da uyumlu hale getirmektedir.

Bir kısım özel dernek ve STK, e-ticaret alanında Uluslararası Tüketici, Uluslararası Tüketici Koruma ve İcra Ağı ve ICC de dahil olmak üzere tüketicinin korunmasına odaklanmaktadır.

E-ticaretin gelecekteki gelişimi, ulusal yasaların (ayrıca) uyumlaştırılmasını ya da e-ticaret müş-teri korumasına yönelik yeni bir uluslararası rejimi gerektirecektir..

www.igbook.info/consumers

Vergilendirme

İnternet ve vergilendirme konusunda tartışma ruhu, Faraday'a, (elektromanyetik indüksiyon) icadının amacını soran şüpheli bir politikacıya verdiği yanıtı benzetilebilir: 'Efendim, bunun ne için olduğunu bilmiyorum. Fakat kesin olarak emin olduğum bir şey var, bir gün bunu vergilendireceksiniz.'⁴⁸

İnternet, modern ekonominin çekirdeği haline geldikçe, vergilendirme konusu daha fazla ele alınmaktadır. 2008'deki mali krizden bu yana daha da önemli hale gelmiştir. Birçok hükümet, artan kamu borcunu azaltmak için mali geliri artırmaya çalışmaktadır. İnternette ekonomik faaliyetlerin vergilendirilmesi, mali gelirin artırılması için ilk fırsatlardan biri haline gelmiştir.

İnternet vergilendirmesi konusundaki ilk kapsamlı raporlardan biri, Fransa Ekonomi ve Maliye Bakanlığı tarafından Ocak 2013'te sunulmuş⁴⁹ ve ardından dijital ekonomideki vergilendirme konusu ile ilgili diğer raporlar gelmiştir.⁵⁰

Siber sorunların gerçek hayattaki sorunlardan farklı bir şekilde ele alınması gerekip gerekmediğine dair İnternet yönetim ikilemi vergi sorununda da açıkça görülmektedir. ABD, ilk günlerden beri, İnterneti vergisiz bir bölge olarak ilan etmeye çalışmaktadır. 1998'de, ABD Kongresi **İnternet Vergi Özgürlüğü Yasası**'nı kabul etmiştir. Bu kanunun uygulanabilirliği konusu birkaç kez uzatıldıktan sonra, ABD Kongresi, 2016 yılında, eyaletler ve yerel yönetimlerin İnternet erişimini vergilendirmesini yasaklayan bir yasa çıkarmıştır. İnternet Vergi Özgürlüğü Yasası'nın kalıcı olarak uzatılmasına ek olarak, önlem aynı zamanda dijital ürün ve hizmetler üzerindeki bazı vergileri de yasaklamaktadır.⁵¹

OECD ve AB, İnternet'in özel vergilendirmeye konu olmaması gerektiği görüşünü desteklemiştir. OECD'nin 1998 **Ottawa İlkeleri**, e-ticaretin vergilendirilmesinin geleneksel ticari faaliyetler için vergilendirme ile aynı prensiplere dayanması gerektiğini belirtmektedir: tarafsızlık, verimlilik, kesinlik ve sadelik, etkinlik, adalet ve esneklik.⁵² Avrupa Komisyonu, 2014'ten gelen

bir raporda, dijital şirketler için özel bir vergi rejimi olmaması gerektiğini yinelemiştir. Aksine, genel kurallar “dijital” şirketlere diğerleriyle aynı olacak şekilde uygulanmalı veya uyarlanmalıdır.⁵³

İnternetin özel vergi işlemlerine tabi olmaması gerektiği görüşünü takiben AB, 2003 yılında AB içinde olmayan e-ticaret şirketlerinden AB içinde mal satmaları halinde KDV ödemelerini talep eden bir düzenleme getirmiştir. AB’nin kararındaki temel motivasyon, AB dışındaki (çoğunlukla ABD’li) şirketlerin, elektronik şirketler de dahil olmak üzere tüm işlemlerde KDV ödemek zorunda olan Avrupa şirketleri üzerinde üstünlüklerinin olmasıydı. Şu anda, AB üyesi olmayan ülkeler aynı stratejiyi benimsemeye başlamışlardır. İnternet kullanıcılarının sayısındaki hızlı artış ve çoğu ABD’de olmak üzere İnternet şirketlerinin kendi ekonomileri içerisinde artması ile birlikte, birçok ülke kendi sınırları içinde kayıtlı olmayan şirketler tarafından sunulan İnternet hizmetlerini vergilendirmeye başlamıştır. Örnekler Rusya⁵⁴ ve Hindistan’dan⁵⁵ İsrail⁵⁶ ve Endonezya’ya⁵⁷ kadar uzanmaktadır.

Çözümlemeyen bir diğer e-vergi konusu, vergilendirmenin yeri sorunudur. Ottawa İlkeleri, “menşe” vergilendirme ilkesi yerine bir “hedef noktayı” gündeme getirmiştir. Bununla birlikte, ABD hükümeti, çoğu e-ticaret şirketi ABD’de yerleşik olduğu için vergilendirme işlemlerinin kendisinde kalmasına büyük ilgi duymaktadır. Buna karşılık, örneğin AB, satıcılardan daha fazla e-ticaret tüketicisine sahip olduğu için hedef vergilendirme ile ilgilenmektedir.

İnternet bağlamında, vergilendirme sadece mevzuatın revize edilmesi amacı olarak değil, aynı zamanda büyük İnternet şirketlerinin vergi kaçakçılığı bağlamında da tartışılmaktadır. Ocak 2016’da, Avrupa Komisyonu, AB’deki şirketlerin karlarını düşük vergili ülkelere kaydırmasını önlemeyi amaçlayan bir Anti Vergi Önleme Paketi sunmuştur. Bunun yayını Google’ın vergi uygulamalarıyla ilgili yükselen tartışmaların ortasında gerçekleşmiştir. İtalyan makamlarına göre, Google 2009 ve 2013 yılları arasında vergiden 227 milyon Avro kurtarmıştır.⁵⁸ Buna ek olarak, İngiltere’de Google ile ulusal vergi makamları arasında 130 milyon £’lık vergi anlaşmasızına ilişkin tartışmalar ortaya çıkmıştır.⁵⁹ Fransa hükümeti Mayıs 2016’da Fransa’nın şirketi 1,6 milyar Avro vergi borcunu ödememekle suçlarken, vergi dolandırıcılığı soruşturmasının bir parçası olarak Google’ın Paris merkezindeki bir arama yapmıştır.⁶⁰ ABD Eğitim Fonu ve Vatan- daşların Vergi Adaleti Kamu Çıkarları Araştırma Grubu tarafından yapılan son bir araştırma, ilk 30 vergi stopajı yapan işletme arasında 10’unun Apple da dahil teknoloji şirketi olduğunu göstermiştir.⁶¹

Bazı ülkeler, altyapı dağıtımında yatırımları teşvik etmek ve yerel e-ticaret şirketlerini artırmak amacıyla İnternet altyapı sağlayıcıları ve/veya çevrimiçi hizmet sağlayıcıları için vergi muafiyetleri getirmektedir. Örneğin Hindistan’da, telekom bakanlığı, BT sektöründeki yatırımları çekmek için büyük projeler için on yıllık bir vergi ‘ertelemesi’ teklif etmiştir.⁶² Çin’de Devlet Konseyi, Çinli ileri teknoloji şirketlerine vergi muafiyetleri sunarak, kurumlar vergisini % 25’ten % 15’e düşürmüştür.⁶³ İngiltere hükümeti, 2016 bütçesinde, hizmetlerini çevrimiçi satan mikro girişimcilere veya İnternet üzerinden evlerini kiralayabilecek kişilere vergi muafiyetleri getirendüzenlemeler yapmıştır.⁶⁴

Son notlar

- 1 Andrew Odlyzko, internetteki fiyatlandırma ve mimarlık sorununu tarihsel bir bakış açısıyla incelemektedir. Antik dünyadan bu yana ulaşım sistemlerinin fiyatlandırmasına dayanarak, mevcut İnternet fiyatlandırma politikasına ilişkin sonuçlar çıkarmaktadır. Daha fazla bilgi için bkz: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. <http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf> [Erişim 25 Ekim 2016].
- 2 World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 29 Ekim 2016].
- 3 The White House (1997) Framework for Global Electronic Commerce. <http://clinton4.nara.gov/WH/New/Commerce/> [Erişim 25 Ekim 2016].
- 4 WTO (1998) Work programme on electronic commerce. http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm [Erişim 25 Ekim 2016].
- 5 European Union (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 Haziran 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031> [Erişim 25 Ekim 2016].
- 6 PFSweb (2015) B2B eCommerce. <http://www.pfsweb.com/PDF/whitepapers/PFSweb-B2B-eCommerce-Whitepaper.pdf> [Erişim 16 Ağustos 2016].
- 7 WTO (no date) GATT and the Goods Council. http://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm [Erişim 25 Ekim 2016].
- 8 WTO (no date) Services trade. https://www.wto.org/english/tratop_e/serv_e/serv_e.htm [Erişim 2 Kasım 2016].
- 9 WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm [Erişim 25 Ekim 2016].
- 10 A “Geçici” olmasına rağmen, moratoryum DTÖ Bakanlar Konferansı tarafından genişletildi. En son bu karar Aralık 2015’teki Nairobi Bakanlar Konferansında alınmış ve 2017 konferansında gözden geçirilmesi kararlaştırılmıştır. WTO Ministerial Conference (2015) Ministerial Decision of 19 December 2015: WT/MIN(15)42 – WT/L/977. https://www.wto.org/english/thewto_e/minist_e/mc10_e/l977_e.htm [Erişim 25 Ekim 2016].
- 11 DTÖ’nün e-ticaret ile ilgili faaliyetleri için bkz. http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm [Erişim 25 Ekim 2016].
- 12 For more information about the USA/Antigua Online Gambling Case, refer to http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [Erişim 25 Ekim 2016].
- 13 Geneva Internet Platform (2016) Report from WTO Public Forum 2016. <http://digitalwatch.giplatform.org/events/wto-public-forum> [Erişim 27 Ekim 2016].
- 14 DTÖ içerisindeki e-ticaret tartışmaları hakkında daha fazla bilgi için bkz. Maciel M (2016) E-commerce in the WTO: the next arena of Internet policy discussions. <https://www.diplomacy.edu/blog/e-commerce-wto-next-arena-internet-policy-discussions> [Erişim 27 Ekim 2016].
- 15 UNCITRAL (1996) Model Law on Electronic Commerce. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [Erişim 25 Ekim 2016].
- 16 United Nations General Assembly (2005) Resolution A/60/20. United Nations Convention on the

- Use of Electronic Communications in International Contracts. http://www.un-citral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html [Erişim 2 Kasım 2016].
- 17 ebXML website. <http://www.ebxml.org/> [Erişim 25 Ekim 2016].
 - 18 UNCTAD (no date) Information Economy Report (series). <http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx> [Erişim 25 Ekim 2016].
 - 19 UNCTAD (no date) eTrade for All: Unlocking the Potential of E-Commerce in Developing Countries. http://unctad.org/en/Pages/DTL/STI_and ICTs/eTrade-for-All.aspx [Erişim 27 Ekim 2016].
 - 20 OECD (1998) Action Plan for Electronic Commerce. [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC\(98\)9/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En) [ac- cessed 27 Ekim 2016].
 - 21 Teleanu S (2016) Digital policy issues emphasised at the G20 Leaders' Summit. <https://www.diplomacy.edu/blog/digital-policy-issues-emphasised-g20-leaders-summit> [Erişim 27 Ekim 2016].
 - 22 APEC (no date) Paperless Trading Individual Action Plan. <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx> [Erişim 25 Ekim 2016].
 - 23 COMESA (2010) Model Law on Electronic Transactions and Guide to enactment. [http://programmes.comesa.int/attachments/article/166/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20\(fin\).pdf](http://programmes.comesa.int/attachments/article/166/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20(fin).pdf) [Erişim 25 Ekim 2016].
 - 24 Net Market Share (2016) Market Share Statistics for Internet Technologies. <https://www.netmarkets-hare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0> [Erişim 1 Eylül 2016].
 - 25 Thuy T, Nguyen T and Armitage GJ (2005) Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model. *ETRI Journal* 27(1) pp. 64–74. <http://etrij.etri.re.kr/etrij/journal/article/article.do?volume=27&issue=1&page=64> [Erişim 25 Ekim 2016].
 - 26 Hayel Y, Maille P and Tuffin B (2005) Modelling and analysis of Internet pricing: introduction and challenges. In *Proceedings of the International Symposium on Applied Stochastic Models and Data Analysis (ASMDA)*, Brest, France. <http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf> [Erişim 26 Ekim 2016].
 - 27 European Commission (2016) A European agenda for the collaborative economy. <http://ec.europa.eu/DocsRoom/documents/16881> [Erişim 1 September 2016].
 - 28 Bkz. Holland K and Cortese A (1995) The future of money: e-cash could transform the world's financial life. *Business Week*, 12 Haziran, p. 66.
 - 29 Bkz. Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. *Pittsburgh Tribune-Review*, 1 April. http://triblive.com/x/pittsburghtrib/business/s_789300.html [Erişim 1 Kasım 2016].
 - 30 Basel Committee on Banking Supervision (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basel March 1998 <http://www.bis.org/publ/bcb35.pdf> [Erişim 25 Ekim 2016]. Final version published in 2003 and <http://www.bis.org/publ/bcb3598.htm> [Erişim 25 Ekim 2016].
 - 31 Kamberi A (2014) Cryptocurrencies and Bitcoin. <https://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin> [Erişim 25 Ağustos 2016].
 - 32 European Central Bank (2012) Virtual currency schemes. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> [Erişim 17 Ağustos 2016].
 - 33 European Banking Authority (2014) EBA Opinion on 'virtual currencies'. <https://www.eba.europa.eu>

- eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [Erişim 17 Ağustos 2016].
- 34 The Register (2016) China to set up its own virtual currency. 22 January. <http://www.theregister.co.uk/2016/01/22/china-virtual-currency-risks/> [Erişim 29 Ekim 2016].
- 35 He D et al. (2016) Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund Staff Discussion Note 16/03. <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> [Erişim 21 Şubat 2016].
- 36 Soxlaw (no date) A guide to the Sarbanes Oxley Act. <http://www.soxlaw.com/> [accessed 26 Ekim 2016].
- 37 European Union (2009) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF> [Erişim 26 Ekim 2016].
- 38 The Basel Group is based at the Bank for International Settlements. It provides a Survey of Developments in Electronic Money and Internet and Mobile Payments. <http://www.bis.org/publ/cpss62.pdf> [Erişim 26 Ekim 2016].
- 39 Richtel M (2002) PayPal and New York in Accord on Gambling. The New York Times, Ağustos 22. <http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm> [Erişim 26 Ekim 2016].
- 40 Takemoto Y and Knight S (2014) Mt. Gox file for bankruptcy, hit with lawsuit. Reuters, 28 February. <http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R00FX20140228> [Erişim 26 Ekim 2016].
- 41 Federal Bureau of Investigation (2014) Press Release: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court> [accessed 26 Ekim 2016].
- 42 Baron J et al. (2015) National Security Implications of Virtual Currency. Examining the Potential for Non-state Actor Deployment. Rand Corporation. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf [Erişim 17 Ağustos 2016].
- 43 European Commission (2016) Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf [accessed 17 Ağustos 2016].
- 44 OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. <http://www.oecd.org/internet/consumer/oecdguidelinesforconsumerprotection-inthecontextofelectroniccommerce1999.htm> [Erişim 26 Ekim 2016].
- 45 OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. http://www.oecd-ilibrary.org/industry-and-services/oecd-guidelines-for-protecting-consumers-from-fraudulent-and-deceptive-commercial-practices-across-borders_9789264103573-en-fr [Erişim 1 Kasım 2016].
- 46 European Union (2001) Regulation (EC) No 44/2001 (Brussels I Regulation). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML> [Erişim 26 Ekim 2016].

- 47 European Union (2012) Regulation (EU) No 1215/2012 (Recast Brussels I Regulation). Avail- able at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:P DF> [Eri- şim 26 Ekim 2016].
- 48 Soete L and Weel B (1999) Cybertax. Maastricht Economic Research Institute on Innovation and Te- chnology (MERIT), Maastricht University. <http://www.merit.unu.edu/pub- lications/rmpdf/1998/rm1998-020.pdf> [Erişim 27 Ekim 2016].
- 49 Collin P and Colin N (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Avail- able at http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf [Erişim 27 Ekim 2016].
- 50 Examples of publications dealing with the issue of Internet taxation include: EY (2015) The dawning of digital economytaxation.[http://www.ey.com/Publication/vwLUAs-sets/ey-the-dawning-of-digi- tal-economy-taxation/\\$FILE/ey-the-dawning-of-digital-economy- taxation.pdf](http://www.ey.com/Publication/vwLUAs-sets/ey-the-dawning-of-digi- tal-economy-taxation/$FILE/ey-the-dawning-of-digital-economy- taxation.pdf) [Erişim 17 Ağustos 2016]; Andes S and Atkinson R (2013) A Policymakers' Guide to Internet Tax. <http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf> [Erişim 17 Ağustos 2016]; OECD (2015) Addres- sing the Tax Challenges of the Digital Economy. http://www.oecd-ilibrary.org/taxation/addres- sing-the-tax-challenges-of-the-digi- tal-economy_9789264218789-en [Erişim 17 Ağustos 2016]. For more resources on this issue, consult GIP Digital Watch observatory (no date). Taxation. <http://digitalwatch.gi- platform.org/issues/taxation> [Erişim 17 Ağustos 2016].
- 51 Phillips Erb K (2016) Congress Makes Internet Access Tax Ban Permanent. Forbes, 11 Şubat. <http://www.forbes.com/sites/kellyphillipserb/2016/02/11/congress-makes-internet-access-tax-ban-perma- nent/#a403c12380a3> [Erişim 26 Ekim 2016].
- 52 The Ottawa Taxation Principles are: Neutrality, Efficiency, Certainty and simplicity, Effective- ness and fairness, Flexibility. OECD (2003) Implementation of the Ottawa Taxation Framework Condi- tions. The 2003 Report. <http://www.oecd.org/tax/administration/20499630. pdf> [Erişim 26 Ekim 2016].
- 53 European Commission (2014) Commission Expert Group on Taxation of the Digital Economy. Brus- sels: European Commission,p.5.http://ec.europa.eu/taxation_customs/sites/taxation/files/resour- ces/documents/taxation/gen_info/good_governance_matters/digital/re- port_digital_economy.pdf [Erişim 4 Temmuz 2016].
- 54 The Moscow Times (2016) Russia State Duma passes Google Tax Law. 15 Haziran. <http://themos- cowntimes.com/articles/russia-state-duma-passes-google-tax-law-53310> [Erişim 4 Temmuz 2016].
- 55 Revanna H (2016) Govt notifies 6% equalization tax on online advertisements. IBT, 31 May. <http://www.ibtimes.co.in/govt-notifies-6-equalisation-tax-digital-ads-take-effect- Haziran-1-680785> [Eri- şim 4 Temmuz 2016].
- 56 The Guardian (2016) Google, Facebook, eBay and other tech firms targeted by new Israeli tax rules. 12 April. <https://www.theguardian.com/technology/2016/apr/11/google-face- book-ebay-tech-fir- ms-israel-tax> [Erişim 4 Temmuz 2016].
- 57 Reuters (2016) Indonesia says Internet giants need to pay tax or face blockages. 29 Şubat. <http://www. reuters.com/article/us-indonesia-tax-internet-idUSKCN0W20QM> [ac- cessed 4 Temmuz 2016].
- 58 Reuters (2016) Italian tax police believe Google evaded 227 million euros in taxes: sources. 28 January. <http://www.reuters.com/article/us-google-italy-tax-idUSKCN0V614L> [Erişim 4 Temmuz 2016].
- 59 Robertson J (2016) Google tax row: what's behind the deal. BBC News, 28 January. <http://www.bbc. com/news/business-35428966> [Erişim 4 Temmuz 2016].

- 60 BBC (2016) Google's Paris HQ raided in tax probe. 24 May. <http://www.bbc.com/news/business-36370628> [Erişim 4 Temmuz 2016].
- 61 McIntyre RS et al. (2015) Offshore Shell Games 2015. <http://www.uspirg.org/sites/pirg/files/reports/USP%20ShellGames%20Oct15%201.3.pdf> [Erişim 4 Temmuz 2016].
- 62 Aulakh G (2016) Budget 2016: Telecom Ministry seeks 10-year tax holiday for Make in India drive. Economic Times, 15 February. <http://economictimes.indiatimes.com/industry/telecom/budget-2016-telecom-ministry-seeks-10-year-tax-holiday-for-make-in-india-drive/articles-how/50988028.cms> [Erişim 4 Temmuz 2016].
- 63 Ren (2016) Beijing offers tax concessions to hi-tech companies. South China Morning Post, 14 Şubat. <http://www.scmp.com/news/china/policies-politics/article/1913172/beijing-offers-tax-concessions-high-tech-companies> [Erişim 4 Temmuz 2016].
- 64 Rampen J (2016) Airbnb hosts get first £1,000 tax free after Budget 2016 shake up. Mirror, 16 March. <http://www.mirror.co.uk/money/airbnb-hosts-first-1000-tax-7568083> [Erişim 17 Ağustos 2016].



Bölüm 6

Kalkınma Sepeti

KALKINMA SEPETİ

Teknoloji (tekerlek, tarım aletleri, matbaa, telgraf gibi), tarih boyunca toplumsal değişimin ana itici gücü olmuştur. Teknolojik gelişmelerin toplumda iyileşmeler getirmesi beklenmektedir. Kalkınma ve teknoloji konusundaki mevcut düşüncelerin kökleri aydınlanma dönemine ve on altıncı ile yirminci yüzyıl arasındaki bilim ve teknolojinin büyümesine kadar uzanmaktadır. Bu düşüncenin temelinde teknoloji ile ilerleme arasındaki bağlantı ve teknolojinin çoğu sosyal problemi çözebileceği fikri yatmaktadır: en basit şekliyle daha fazla teknolojinin daha fazla kalkınmaya yol açması gerekmektedir.

Teknoloji ayrıca, ilk kez İkinci Dünya Savaşı'ndan sonra, yeni sömürgelerin, eski sömürgelerin gelişimini destekleme yönünde teşvik edilen BM kalkınma gündemini de şekillendirmiştir. Teknoloji, yoksulluğun azaltılmasına ve birçoğunun refahının iyileştirilmesine katkıda bulunurken, aynı zamanda sınırlamalar ile karşı karşıya kalmıştır. Sosyal ve ekonomik gelişmeler teknolojik gelişmelerden çok daha karmaşıktır. Örneğin, bireylerin yeni teknolojilerden yararlanmasında ve aynı zamanda, hem yerel kültürlerin hem de modern gelişmelere adapte etme gerekliliğini yansıtan politika ve kurumların güçlendirilmesi yönünde eğitim ve kapasite geliştirme gerekmektedir. Ayrıca, sosyal düzenlemeler zaman gerektirir, çünkü toplum teknolojinin gelişiminden daha yavaş değişir.

Komünizm ve teknolojik güdümlü kalkınmanın başarısızlığı

Teknolojik güdümlü gelişimin en büyük tarihsel başarısızlığı, yirminci yüzyılın sonundaki Komünist sistemin başarısızlığıydı. Bilim ve teknoloji, Sovyetler Birliği ve Doğu Bloku'nun en öncelikli alanlarıydı. Daha sonra başlamasına ve sınırlı kaynaklarına rağmen, Sovyetler Birliği, Batı dünyasının birçok bilimsel ve teknolojik gelişme alanındaki kazanımlarını eşleştirmeyi başardı. Özellikle uydur ve askeri teknolojilerde çok başarılı oldu. Bununla birlikte, teknoloji sosyoekonomik sorunları ele almak için yeterli değildi ve sistem çöktü. İdeolojik ve yapısal olanlar dahil çöküşün birçok nedeni vardır. Bununla birlikte, halen araştırılmakta olan bir neden, teknolojik çözümlere ve teknik mühendisliğe olan ağır bağımlılıktır.

Dijital çağ, teknolojinin olanak sağlayan gücünü bir kez daha tekrarlamıştır. Bireyden küresel düzeye kadar İnternet'in birçok şeyi nasıl sağladığına dair sayısız örnek bulunmaktadır. Ancak, teknolojik ve sosyal ilerleme arasındaki bağlantı, pek çok çalışma ve raporda açıkça belirtildiği gibi otomatik değildir.¹ Teknoloji ve toplum arasındaki karmaşık etkileşim bu bölümde ele alınacaktır. Temel soruların bazıları şunlardır:

- İnternet, gelişmiş ve gelişmekte olan dünyalar arasındaki mevcut uçurumu azaltacak veya genişletecek mi?
- Gelişmekte olan ülkeler, endüstriyel olarak gelişmiş ülkelerin dijital seviyelerine nasıl ve ne zaman ulaşabilecekler?
- İnternet ve dijital teknolojiler farklı boyutlarda sürdürülebilir kalkınmayı nasıl sağlayabilir?

Bu bölüm ana gelişme sorunlarını ele almaktadır. Bununla birlikte, birçok dijital politika tartış-

masında gelişme yatay olarak görünmektedir. Hemen hemen her İnternet yönetişimi konusu, aşağıdaki birkaç örnekte belirtildiği gibi, gelişimsel bir görünüme sahiptir:

- İnternete erişim - dijital bölünmenin üstesinden gelmenin ilk şartı olan internete erişim esas olarak telekomünikasyon altyapısının varlığına bağlıdır.
- İnternet erişimi için mevcut ekonomik model, gelişmekte olan ülkelerde, gelişmiş ülkelerde bulunan omurgalara erişimi finanse etmek zorunda olanlara orantısız bir yük getirmeye devam etmektedir.
- E-ticaret gelişmekte olan ülkelerdeki şirketlere küresel pazara erişimleri için fırsatlar sunmaktadır, ancak bu tür şirketlerin önce İnternet'e erişmesi gerekmektedir.

Dijital teknolojiler ve kalkınma: politika çerçeve

2000'li yılların başlarında WSIS sürecinde, küresel kalkınma gündemine dijital kalkınma sorunları konulmuştur. WSIS hakkındaki ilk UNGA kararı, WSIS'in "özellikle teknolojiye erişim ve teknoloji transferi konusunda gelişmeyi teşvik etmedeki" rolünü vurgulamıştır.² Bu nedenle, zirvenin genel amacı, gelişmiş ve gelişmekte olan ülkeler arasındaki dijital uçurumun köprülenmesine katkıda bulunmak ve milenyum kalkınma hedeflerinin (Milenyum Kalkınma Hedefleri) uygulanmasını kolaylaştırmaktır. WSIS [Cenevre Deklarasyonu ve Eylem Planı](#), kalkınmayı öncelik olarak vurgulamış ve onu [BM Milenyum Deklarasyonu](#)³ ile bütün ülkelerin kalkınma için bilgi, bilgi ve iletişim teknolojilerine erişiminin tanıtımına bağlamıştır. Milenyum Kalkınma Hedefleri'yle⁴ ilişkili olarak WSIS kalkınma bağlamında güçlü bir şekilde konumlandırılmıştır. [Tunus Bilgi Toplumu Gündemi](#) ayrıca, kalkınma için BİT ile ilgili meseleleri ele almış, belgenin önemli bir kısmı ilgili zorlukların üstesinden gelmek için finansal mekanizmalara adanmıştır. On yıldan uzun bir süre sonra, UNIS'in üst düzey toplantısının, WSIS sonuçlarının uygulanmasının genel incelemesine ilişkin sonuç belgesinin (WSIS + 10 çıkış belgesi), 5. Maddesinde WSIS ve [SDG'ler](#)⁵ arasında bir bağlantı oluşturduğu görülmüştür:

Bağlantının, inovasyonun ve erişimin artmasının Milenyum Kalkınma Hedefleri'nde ilerleme sağlamada kritik bir rol oynadığını kabul ediyoruz ve Bilgi Toplumu Süreci Dünya Zirvesi ile 2030 Sürdürülebilir Kalkınma Gündemi arasında çapraz kesimi vurgulayarak bilgi ve iletişim teknolojisinin Sürdürülebilir Kalkınma Hedefleri'ne ve yoksulluğun ortadan kaldırılmasına olan katkısı, bilgi ve iletişim teknolojilerine erişimin kendi başına bir gelişme göstergesi ve özlemi haline geldiğine dikkat çekmek istiyoruz.⁶

Milenyum Kalkınma Hedefleri, Hedef 9'da İnternet'e doğrudan atıfta bulunmaktadır; bu hedef, 'BİT'e erişimi önemli ölçüde artırmak ve LDC'lerde 2020'ye kadar İnternet'e evrensel ve uygun fiyatlı erişim sağlamak' yönündedir. Ayrıca, SDG'ler çerçevesinde, bilim, teknoloji ve inovasyonun SDG'lerin elde edilmesini nasıl kolaylaştıracağını inceleyen Teknoloji Kolaylaştırma Mekanizması kurulmuştur.⁷

Geliştirme teması ayrıca, Atina'daki (2006) ilk toplantısından başlayarak, 2015'teki en son IGF'ye kadar, genel temanın "İnternet Yönetişiminin Evrimi: Sürdürülebilir Kalkınmanın Güçlendirilmesi" olduğu, IGF içerisinde de vurgulanmıştır.

BİT toplumun gelişimini nasıl etkiler?

SKH'lerin kabul edilmesinin ardından, bu soruyu incelemeyi ve BİT'lerin kalkınmaya katkı sağlamasının yollarını araştırmayı amaçlayan birçok girişim olmuştur.

Bazı örnekler arasında UNCTAD'ın Kalkınma için ICT programı⁸; BİT'in farklı SDG'lere⁹ katkıda bulunma yollarını özetleyen WSIS Eylem Hatları - SDG Matrisi; ve SDG'leri BİT çözümlerine bağlamayı amaçlayan WSIS Forumu'nun 2015 ve 2016 sürümleri gösterilebilir.¹⁰ Son olarak, CSTD, 2015-2016 dönemindeki oturumlararası etkinliğini, ekonomi, toplum ve çevre konularında (NesNet, çevrimiçi eğitim, 3D baskı, dijital otomasyon gibi teknolojiler dahil olmak üzere) son dijital uygulamaların potansiyel uzun vadeli etkilerini inceleyen "Dijital kalkınma öngörüsü" temasına odaklanmıştır. Komisyon, hükümetlere insan sermayesi, BİT ve tamamlayıcı altyapı ve yasal çerçevelere odaklanarak diğerlerinin yanı sıra, ortaya çıkan teknolojilerin gelişimini destekleme ve yarattıkları fırsatlardan yararlanma, dijital gelişim için olanak sağlayan bir ortamın teşvik edilmesi ve bu alanlara odaklanılması için uygun politikalar benimsemeleri konusunda çeşitli önerilerde bulunmuştur.

Dünya Bankası'nın [2016 Dünya Kalkınma Raporu: Dijital Paylar](#)¹¹, BİT ile kalkınma arasındaki bağlantının tartışılmasına ihtiyati bir yaklaşım getirerek, daha fazla teknolojinin daha fazla kalkınmaya yol açacağına dair basit bir görüşü sorgulamıştır. Rapor, İnternet (ve daha geniş bir anlamda dijital teknolojiler) büyüme ve gelişmeyi mümkün kılma potansiyeline sahip olmasına rağmen, eşitsizliklerin ve boşlukların hem küresel düzeyde hem de ülkeler arasında var olmaya devam etmesi ve hatta artması dikkat çekicidir.

Dijital teknolojiler, insanlara (bilgiye, işlere ve diğer fırsatlara daha kolay erişim gibi), işletmelere (daha fazla üretkenlik ve ticaret, daha fazla rekabet ve yenilikçilik gibi) ve hükümetlere (daha iyi kamu hizmetleri ve vatandaşlarla daha iyi etkileşim gibi) faydalar sağlar. Ancak bu faydalar, gerçek küresel ekonomik büyümeye izin verecek kadar ve hızla yayılmamaktadır. Bu zorluğun üstesinden gelmek için, Dünya Bankası raporu iki ana yön önermektedir: dijital uçurumu kapatmak; ve bireysel kullanıcıların, iş dünyasının ve kamu sektörünün dijital teknolojilerden tam anlamıyla yararlanmalarını sağlayacak tamamlayıcı politikalar geliştirmek. Topluca analog tamamlayıcılar olarak bilinen bu tür politikalar piyasa rekabetini ve şirketleri sürekli yenilik yapmaya teşvik eden düzenlemeleri, dijital okuryazarlık alanındaki eğitim ve öğretim programlarına odaklanan politikaları, teknolojiyi politika yapma süreçlerinde ve kamu hizmetlerinin sunulmasında etkin biçimde kullanan daha yetenekli ve hesap verebilir kamu kurumları kapsar. Üstelik, tüm bu bileşenler mevcut olsa bile, temel zorluk, bunların nasıl ve ne zaman kullanılacağı ve birleştirileceği ile ilgilidir.

Rapor, teknolojinin asla tarafsız olmadığı eski düşüncesini bir kez daha doğrulamıştır. İnsan toplumunun tarihi, bazılarını hariç tutarken bazı bireyleri, grupları veya ulusları güçlendiren birçok teknoloji örneği sunmaktadır. İnternet bu açıdan farklı değildir: bireyden küresel düzeye kadar dijital fırsatlar farklı şekillerde ele geçirilir ve zenginlik ve güç dağılımında köklü bir değişim meydana gelmiştir.

Kısacası, BİT'in sosyo-ekonomik kalkınma üzerindeki etkileri karmaşık ve geniş kapsamlıdır. Bununla birlikte, BİT'lerin bu sosyal ve ekonomik boyutlarına artan ilgi, BİT ağının toplum

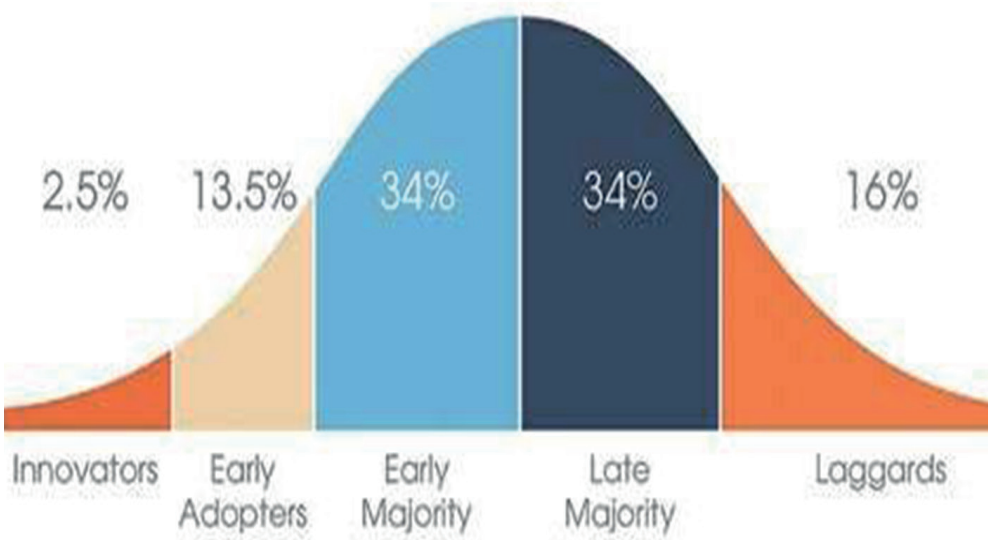
üzerindeki etkisinin daha iyi ölçmek ve çözmek ve sosyo-ekonomik kalkınma için BİT uygulamalarını en iyi şekilde nasıl kullanabileceğini bulmak için imkanlar sunmaktadır.

www.igbook.info/development

Dijital uçurum

Dijital uçurum, BİT/İnternete erişme ve kullanma kapasitesine sahip olanlar ile, teknik, politik, sosyal veya ekonomik nedenlerle BİT/interneti kullanamayanlar arasındaki boşluk olarak tanımlanabilir. OECD, dijital uçurumu “hem bilişim, hem iletişim, hem de bilişim teknolojilerine (BİT) erişim imkânları ve interneti geniş bir faaliyet çeşitliliğinde kullanma imkânları açısından farklı sosyoekonomik seviyelerdeki bireyler, haneler, işletmeler ve coğrafi alanlar arasındaki boşluk” olarak adlandırılmaktadır.¹²

Dijital uçurum bağımsız bir fenomen değildir. Eğitim, sağlık, sermaye, barınak, istihdam, temiz su ve gıdadaki mevcut sosyo-ekonomik eşitsizlikleri yansıtmaktadır.



Şekil 21. Rogers'ın yeniliklerin yayılması eğrisi

Rogers'ın yeniliklerin yayılması eğrisi (Şekil 21), teknolojik araçların sunduğu olanaklar ile teknoloji algısı ve benimseme gerçekleri arasındaki kritik etkileşimi açıklamaya yardımcı olmaktadır. Yenilikçilerden yavaş kalanlara kadar teknolojilerin uygulayıcılarını çeşitli kategorilerde sınıflandırmaktadır.

Rogers'ın eğrisi aynı zamanda ülkeler içinde ve ülkeler arasında, kırsal ve kentsel nüfus arasında, yaşlı ve genç arasında, kadın ve erkek arasında, eğitilmiş ve az eğitilmiş olanlar arasında farklı düzeylerde var olan dijital uçurumları da açıklar.

Dijital uçurum genişliyor mu?

BİT/İnternet gelişmeleri, gelişmekte olan dünyayı diğer alanlardaki gelişmelerden (örn. Tarımsal veya tıbbi teknikler) çok daha hızlı bir şekilde geride bırakmaktadır ve gelişmiş dünyanın bu teknolojik gelişmelerden başarıyla yararlanmak için gerekli araçlara sahip olması nedeniyle, dijital uçurum sürekli ve hızla genişlemektedir. Bu görüş, Birleşmiş Milletler Kalkınma Programı (UNDP) [İnsani Gelişme Raporları](#) ve Uluslararası Çalışma Örgütü (ILO) [Küresel İstihdam Raporları](#) gibi çeşitli saygın belgelerde dile getirilmektedir.

Bazı muhalif görüşler, dijital uçurumdaki istatistiklerin çoğu zaman yanıltıcı olduğunu ve dijital uçurumun aslında hiç de genişlemediğini, hatta daraldığını iddia etmektedir.¹³ Bu görüşe göre, bilgisayar sayısına, İnternet web sitelerinin sayısına veya mevcut bant genişliğine olan geleneksel odaklanma, BİT/İnternet'in gelişmekte olan ülkelerdeki toplumlar üzerindeki daha geniş etkilerine odaklanarak değiştirilmelidir. Sık alıntı yapılan örnekler Brezilya, Çin ve Hindistan'ın dijital başarılarıdır.

Aslında, dijital uçurumdaki boşlukları değerlendirme kriterleri gelişme gerçeklerini daha iyi yakalamak için değişmekte ve daha karmaşık hale gelmektedir. Mevcut değerlendirmeler, BİT'e hazırlık ve toplum üzerindeki genel BİT etkisi gibi yönleri ele almaktadır. WEF, [Ağa Hazırlık Endeksi](#)'ni (NRI), dünyadaki ülkelerin İnternet seviyesini ölçmede yeni bir yaklaşım olarak geliştirmiştir.¹⁴ Ayrıca, dijital uçurumun nasıl ele alınacağına dair yeni bakış açıları sağlamaktadır.

Evrensel erişim

Dijital uçuruma ek olarak, kalkınma tartışmalarında sıkça bahsedilen bir diğer kavram [evrensel erişimdir](#), yani herkes için internet erişimidir. Her ne kadar herhangi bir dijital kalkınma politikasının temel taşı olsa da, evrensel erişimin doğası ve kapsamı ile ilgili farklı algı ve anlayışlar devam etmektedir. Küresel düzeyde evrensel erişim sorunu, büyük ölçüde açık bir sorun olmaya devam etmektedir ve temel olarak gelişmiş ülkelerin bu hedefin gerçekleştirilmesine yatırım yapmaya hazır olmasının yanı sıra, gelişmekte olan ülkelerdeki politika ortamına da bağlıdır. Yine de, evrensel erişimin önemi, WSIS + 10 sonuç belgesi gibi birçok uluslararası belgede ifade edilmiştir.

Küresel düzeyde evrensel erişimin aksine, bazı ülkelerde evrensel erişim oturmuş bir ekonomik ve yasal kavramdır. Tüm vatandaşlara telekomünikasyon erişimi sağlamak ABD telekomünikasyon politikasının temelidir. Sonuç, uzak bölgelerdeki ve yüksek bağlantı maliyetlerine sahip bölgelerdeki erişim maliyetlerini sübvansiyon etmek için gelişmiş bir politika ve finansal mekanizma sistemidir. Sübvansiyon, büyük şehirler olmak üzere düşük bağlantı maliyeti olan bölgeler tarafından finanse edilmektedir. AB ayrıca, her vatandaşın bir İnternet bağlantısı da dahil olmak üzere temel iletişim hizmetlerine erişmesini ve belirli düzenlemeleri yürürlüğe sokmasını sağlamak için politikaları teşvik ederek evrensel erişime ulaşmak yolunda bazı somut adımlar

atmıştır.¹⁵ Eylül 2016'da Avrupa Komisyonu tarafından öne sürülen Avrupa Elektronik Haberleşme Kanunu'na ilişkin bir teklif, (kamu ankesörlü telefonları gibi) eski hizmetleri kapsama alanından kaldırarak ve geniş banda odaklanarak, AB'de evrensel hizmet kavramını yeniden tanımlamayı planlamaktadır.¹⁶

Son zamanlarda, birçok İnternet şirketi İnternet erişimini artırmak için girişimlerde bulunmaktadır. Henüz bağlı olmayan bölgelerin muazzam ticaret potansiyelini toplamaya çalışmaktadır. Bu girişimler ya geleneksel kablo oluşturma araçlarına odaklanmakta ya da (Facebook gibi) İnternet yayıcı dronları ve (Google gibi) internet yayıcı balonları kullanmak gibi geleneksel olmayan yöntemlere dayanmaktadır.

Yenilikçi çözümler de dahil internet alt yapısına ilişkin daha fazla tartışma için Bölüm 2'ye bakınız.

Dijital uçurumu aşma stratejileri

Bir UNHRC raporunun¹⁷ işaret ettiği gibi, erişimin altyapıya erişimden içeriğe erişime kadar farklı boyutlar içerdiği için, dijital uçurumun üstesinden gelmek, küresel, bölgesel ve ulusal düzeyde karma önlemler ve çok sayıda aktörün (hükümetler, hükümetlerarası kuruluşlar, özel sektör gibi) dahil olacağı politikalar gerektiren karmaşık ve uzun vadeli bir süreçtir.

Telekomünikasyon ve internet altyapılarının geliştirilmesi

İnternet altyapısına erişim, dijital uçurumun üstesinden gelmenin en büyük zorluklarından biridir. Gelişmekte olan ülkelerde internete erişim ile ilgili iki ana husus vardır. Birincisi, uluslararası İnternet omurgalarına erişimdir. İkincisi, gelişmekte olan ülkelerdeki bağlantıdır.

Uluslararası İnternet omurgalarına erişim, esas olarak, kıtaların bağlanması önemli bir rol oynayan denizaltı fiber optik kabloların mevcudiyetine bağlıdır. Coğrafya nedeniyle, aynı zamanda nispeten düşük dağıtım maliyetleri nedeniyle, büyük kıtalararası bel kemiği bağlantıları okyanusların altında kalmaktadır. Bu kablolar şu anda tüm küresel İnternet trafiğinin% 90'ından fazlasının aktığı ortamı sağlamaktadır.

İnternet omurga kabloları konusunda daha fazla tartışma için Bölüm 2'ye bakınız.

Denizaltı kablolarına ek olarak, ek karasal kıtalararası kablolar için yeni planlar ortaya çıkmaktadır. Örneğin Tek Çin Kemer, Tek Yol projesi, Asya ve Avrupa'yı birbirine bağlamak için bir fiber optik karasal kablo dağıtımını planlamaktadır. Daha fazla karasal bağlantı kablosu planlama aşamasındadır.

Uzun vadede, karasal İnternet iletişimine doğru kayma, karadaki Avrasya ülkeleri üzerinde gelişimsel bir etki yaratabilir. İnternet denizaltı kabloları yoluyla pahalı bir erişimi finanse etmeleri

gereken mevcut duruma kıyasla, İnternet'e daha kolay ve daha ucuz erişim sağlanabilir.

Gelişmiş erişim için başka bir çözüm, yerel trafiği bir ülke içinde tutmaya yardımcı olan IXP'lerin gelmesidir. Örneğin, IXP'ler olmadan, aynı ülkedeki iki operatörün müşterileri arasındaki e-posta alışverişi genellikle uluslararası bağlantı yoluyla yönlendirilir ve aynı ülkeye geri gönderilirdi. IXP'ler, farklı ISS'lerin internet trafiğini eşleştirme yoluyla (ödeme yapmadan) değiştirdikleri teknik tesislerdir. IXP'ler genellikle İnternet trafiğini (şehir, bölge, ülke gibi) daha küçük alanlarda tutmak için kurulur.

Yine de, gelişmekte olan birçok ülkede IXP yoktur, bu da ülke içindeki müşteriler arasındaki trafiğin önemli bir kısmının başka bir ülkeye yönlendirildiği anlamına gelir. Bu, gelişmekte olan ülkeden uzun mesafeli uluslararası veri trafiğinin hacmini ve ülkeye İnternet servisi sağlama maliyetini artırmaktadır. Farklı girişimler, gelişmekte olan ülkelerde IXP'leri kurmaya çalışmaktadır.¹⁸ Önemli başarılar elde edenlerden biri, AU'nun Afrika'da IXP'lerin kurulmasını destekleyen Afrika İnternet eXchange Sistemi (AXIS) Projesi'dir.

Gelişmekte olan ülkelerdeki bağlantı bir başka önemli zorluktur. Daha önce, İnternet kullanıcılarının çoğunluğu büyük şehirlerde yoğunlaşmıştı. Kırsal alanların genellikle internete erişimi yoktu. Mobil telefon ve kablosuz iletişimin hızlı büyümesiyle durum değişmeye başlamıştır.

Kablosuz iletişim, çoğu zaman zorlukları olan (birçok Asya ve Afrika ülkesinde çok uzun mesafelerde kablo döşenmesi içeren) geleneksel karasal iletişim altyapılarının gelişimine uygun bir alternatif olabilir. Bu bağlamda, radyo spektrum politikaları, spektrum kullanılabilirliği ve verimli kullanımın sağlanmasında büyük öneme sahiptir. Bu şekilde, daha hızlı İnternet gelişiminin önündeki en büyük engellerden biri olan yerel ağın paylaşıma açılması veya yerel ağ döngü problemi aşılabılır. Bununla birlikte, mobil teknolojilerin kapsamlı bir çözüm olmadığı, ancak bağlantı eksikliği olan geniş alanları kapsayan bir aracı olduğu konusunda da görüşler bulunmaktadır. Radyo spektrumunun, örneğin kablosuz ağlar üzerinden bağlanabilen cihazların sayısı ile ilgili fiziksel sınırlara sahip olduğu da iddia edilmektedir.¹⁹

Geleneksel olarak, dijital uçurumun altyapısal yönü, ITU - D aracılığıyla ITU'nun odak noktası olmuştur.

Gelişmekte olan ve gelişmiş ülkeler arasındaki bağlantıların maliyetini kim karşılamalı?

Afrika'daki bir son kullanıcı Avrupa, ABD veya Çin'deki bir muhabire e-posta gönderdiğinde, Afrika ISS'i Afrika'dan Avrupa'da, Kuzey Amerika ve Asya'daki ana İnternet merkezlerinde bulunan ana omurgalara uluslararası bağlantı maliyetini taşımaktadır. Bununla birlikte, bir Avrupalı son kullanıcı Afrika'ya bir e-posta gönderdiğinde, Afrika ISS hala uluslararası bağlantının maliyetini üstlenir ve nihayetinde Afrika son kullanıcısı iki yönlü dijital trafik akışını kapsayan daha yüksek abonelik ücretleri ödeyerek asıl yükü üstlenir. Bunun sebebi, gelişmekte olan ülkelerdeki ISS'lerin, küçük müşteri tabanları nedeniyle, büyük uluslararası tedarikçilerle paylaşılan maliyet eşleştirme anlaşmalarına girmekte zorluk çekmeleridir. Bu ISS'ler sonuçta daha yüksek maliyetlerle uluslararası sağlayıcılardan bağlantı satın almaları ve yerel müşterilerine satmaları nedeniyle satıcı gibi davranırlar.²⁰

İnternet ücretlerinin mevcut sistemindeki değişikliklerle ilgili tartışmalardaki ana argüman, iletişim uç noktaları arasındaki maliyetleri ve gelirleri paylaşan telefon finansal uzlaştırma sisteminin benzetmesini kullanmaktadır. Bununla birlikte, APNIC'in Baş Bilimcisi Geoff Huston, bu benzetmenin sürdürülebilir olmadığını savunmaktadır.²¹ Telefon sisteminde, iki telefon seti arasındaki telefon sohbetinin net bir şekilde tanımlanabilir bir emtia bedeli vardır. İnternet eş-değer, tek bir metaya sahip değildir; ağ üzerinden farklı yollar alan paketlere sahiptir. Bu temel fark telefonla analogiyi uygunsuz kılmaktadır. Aynı zamanda, telefon finansal çözüm modelinin İnternete uygulanamamasının temel nedenidir.

ITU, İnternet erişiminin daha dengeli bir şekilde dağıtılmasını hedefleyen İnternet giderlerinin çözümünde mevcut sistemde olası iyileştirmeler hakkında tartışmalar başlatmıştır. 2008 yılında, uluslararası internet bağlantılarıyla ilgili ticari anlaşmalar için taraflar arasında trafik akışı, rota sayısı, uluslararası iletim maliyeti gibi unsurların değeri için tazminat gerekliliğini göz önünde bulunduracak tavsiyeleri içeren ITU [Tavsiye Kararı D.50](#) kabul edilmiştir. Gelişmiş ülkelerden ve telekom operatörlerinden gelen muhalefet nedeniyle, öneri pratik olarak etkisiz olmuştur. Hükümetler arasında bu konuyu müzakere etmenin sınırlamalarından biri, ara bağlantı anlaşmalarının çoğunun özel telekomünikasyon operatörleri arasında yapılması ve genellikle gizli kalmasıdır. Bu, ITU'nun 2013 yılında IXP'ler, denizaltı kablolarının piyasaya sürülmesi ve yerel içeriğin geliştirilmesi gibi uluslararası İnternet bağlantısının maliyetini düşürmek için alternatif yöntemleri vurgulayan [D.50 Tavsiye Kararı Ekini](#) kabul etmesini sağlamıştır.²²

Mali destek

WSIS sürecinde, dijital uçurumun köprülenmesi için finansal desteğin önemi açıkça anlaşılmıştır. WSIS'de önerilen bir fikir, teknolojik açıdan dezavantajlı ülkelerin telekomünikasyon altyapıları inşa etmelerine yardımcı olmak için BM tarafından yönetilen bir Dijital Dayanışma Fonunun kurulmasıydı. Küresel Dijital Dayanışma Fonu, Mart 2005'te resmen başlatılmış olmasına rağmen, merkezi bir kalkınma fonu kurulması yerine doğrudan yatırımları tercih eden gelişmiş ülkelerden geniş destek görmemiştir.

Gelişmekte olan ülkeler, UNDP veya Dünya Bankası gibi ikili veya çok taraflı kalkınma ajansları, bölgesel kalkınma girişimleri ve bankalar gibi çeşitli kanallardan finansal destek almaktadırlar. ITU ayrıca, ulusal, bölgesel ve küresel düzeyde BİT gelişimi ile ilgili projelerin uygulanması yoluyla sürdürülebilir kalkınmanın teşvik edilmesine katkıda bulunmayı amaçlayan bir başlangıç finansmanı girişimi olan BİT Geliştirme Fonu başlatmıştır. İleriye baktığımızda, Uluslararası Kalkınma Finansmanı Konferansı'nda kabul edilen ve Temmuz 2015'te UNGA'nın onayladığı [Addis Ababa Eylem Gündemi](#), tüm SDG'lerde dijital uçurumun çeşitli boyutlarını kapatılması için ülkelerin finansal desteğini teşvik edebilecek sürdürülebilir kalkınmanın finanse edilmesi için küresel bir çerçeve sunmaktadır.²³

Telekomünikasyon piyasasının artan serbestleşmesi ile birlikte, doğrudan yabancı yatırımlarla telekomünikasyon altyapıları geliştirme eğilimi artmıştır. Gelişmiş ülkelerin telekomünikasyon piyasaları aşırı doygun hale geldiğinden, birçok uluslararası telekomünikasyon şirketi gelişmekte olan ülkelerin pazarlarını gelecekteki büyüme için bir alan olarak görmektedir.

Etkili erişim için beceri ve yeterlilikler

İnternete bağlanmak için temel yetenek, erişim için bir ön koşuldur. Yine de, erişimin tanımının, bazıları tarafından önemli ölçüde daha geniş olduğuna ve erişimin kalitesini dikkate alması gerektiğine inanılmaktadır. WSIS + 10 sonuç belgesi, bu bağlamda, erişimi neyin oluşturduğuna dair gelişen ve bu erişimin kalitesini vurgulayan bir anlayışa dayandığını iddia eder. [...] Hız, istikrar, uygun fiyat, dil, yerel içerik ve engelliler için erişilebilirlik artık kalitenin temel unsurlarıdır.

İletişim altyapısının varlığı, insanlar İnternet'e erişmek ve İnternet'ten yararlanmak için araçlara (cihazlara) ve bilgiye (BİT okuryazarlığı) sahip olmadıkça işe yaramaz. Gelişmekte olan ülkeler, özellikle de Afrika'daki ülkeler, küresel çevrimiçi bilgiye sınırlı bir katkıda bulunmaktadır. Gelişmiş ve gelişmekte olan dünya arasındaki boşluk, örneğin internete erişimde, bilgi katkısı konusunda daha belirgindir. Örneğin, Hong Kong (SAR Çin), Wikipediada, Afrika 50 kat daha fazla İnternet kullanıcısına sahip olmasına rağmen, tüm Afrika'dan daha fazla içerik sağlamaktadır.²⁴

Birçok girişim ve organizasyon, becerileri geliştirmeyi amaçlamakta ve dijital uçurumun sosyo-kültürel yönlerine vurgu yapmaktadır. Örneğin, Çocuk Başına Bir Dizüstü Bilgisayar, Boşluğu Kapat ve Uluslararası Bilgisayar Yardımı gibi uluslararası girişimler ve kuruluşlar, gelişmekte olan ülkelerdeki hizmetsiz topluluklara yenilenmiş ve düşük maliyetli ekipman sağlamayı amaçlamaktadır. Uygun fiyatlı cihazlar sağlama konusunda yerel girişimler de başlatılmıştır. Örneğin Singapur, düşük gelirli ailelerden gelen engelli öğrencilere ve öğrencilere uygun bir fiyata bilgisayarı edinme fırsatı veren bir programa sahiptir.²⁵

Gelişmekte olan ülkeler için en önemli konulardan biri yüksek vasıflı emeğin gelişmekte olan ülkeden gelişmiş ülkelere hareketi anlamına gelen beyin göçüdür. Beyin göçü ile gelişmekte olan ülkeler göç eden yetenekli emeğin eğitim ve öğretimine yaptıkları yatırımlarının yanı sıra yetenekli emeği de kaybederler.

ABD ve diğer gelişmiş ülkelerde yetenekli, özellikle de BİT tarafından eğitilmiş işgücünü çekecek çeşitli istihdam ve göç programları dikkate alındığında, beyin göçü büyük olasılıkla devam edecektir.

Öte yandan, durdurabilen veya bazı durumlarda bile beyin göçünü tersine çevirebilecek bir gelişme, BİT işlemlerinin gelişmekte olan ülkelere dış kaynak kullanımı yoluyla teminindeki artıştır. En başarılı örnek, Hindistan'ın Bangalore ve Hyderabad gibi yazılım endüstrisi merkezlerinin geliştirilmesidir.

Politika ve kurumsal yönler

Telekomünikasyon politikası konuları, dijital uçurumun üstesinden gelmekle birçok açıdan yakından bağlantılıdır:

- Ne özel yatırımcılar ne de giderek artan bir şekilde kamu bağışları, İnternet gelişimi için uygun bir kurumsal ve yasal ortamı olmayan ülkelerde yatırım yapmaya hazır değildir.

- Ulusal BİT sektörlerinin gelişimi, gerekli düzenleyici çerçevelerin oluşturulmasına bağlıdır.
- Telekomünikasyon politikası, daha fazla rekabet, daha düşük maliyet ve daha geniş bir hizmet yelpazesi ile verimli bir telekomünikasyon pazarının kurulmasını kolaylaştırmalıdır.

Etkinleştirici bir ortamın yaratılması, telekomünikasyon pazarının kademeli olarak serbest bırakılmasını gerektiren zorlu bir görevdir; İnternet ile ilgili yasaların getirilmesi (telif hakkı, gizlilik, e-ticaret vb.); ve İnternet erişiminin politik, dini veya diğer kısıtlamalar olmadan herkese sunulması gibi.

İlk adımlardan biri, bağımsız ve profesyonel telekomünikasyon düzenleyici makamların kurulmasıdır. Gelişmiş ülkelerden edinilen deneyimler, katı düzenleme stratejilerinin telekomünikasyon altyapısında hızlı bir büyüme için ön koşul olduğunu göstermektedir. Gelişmekte olan ülkeler bu yaklaşımı izlemeye başlamıştır, ancak bazıları hala genel olarak zayıf, bağımsızlık eksikliği olan veya genellikle devlete ait telekom operatörlerinin düzenleyici ve politik süreçlerde etkili olduğu bir sistemin parçası olan düzenleyici otoritelerle sorunlar yaşamaktadır.

Diğer bir önemli zorluk telekomünikasyon pazarının serbestleştirilmesi olmuştur. Hindistan ve Brezilya, genellikle bu tür serbestleşmenin İnternet ve BİT sektörünün hızlı büyümesini kolaylaştırdığı ve genel ekonomik büyümeye fayda sağladığı gelişmekte olan ülkelere örnek olmaktadır. Diğer bazı ülkeler, özellikle en az gelişmiş ülkeler telekomünikasyon pazarının serbestleşmesinin büyük bir zorluk olduğunu düşünmektedir. Telekomünikasyon tükellerinin kaybıyla, bu ülkelerdeki hükümetler önemli bir bütçe geliri kaynağını kaybetmiştir. Düşük bütçe, sosyal ve ekonomik yaşamın diğer tüm sektörlerini etkilemektedir.

Bazı durumlarda, telekom gelirlerini kaybetmekle aynı zamanda, bu ülkeler liberalleşmenin faydalarını daha düşük maliyetlerle ve daha iyi telekom hizmetleriyle elde edememişlerdir, çünkü esas olarak telekomünikasyon şirketlerinin özelleştirilmesi etkin piyasa ve rekabetin kurulması anlamında desteklenmemiştir. Bu tür uygulamalar, Dünya Bankası'nı, ülkelerin devlete ait işletmecilerin özelleştirilmesinden önce veya aynı zamanda özelleştirmeleri sırasında piyasa katmanlarının rekabete açması gerektiğini; bu şekilde, ilk önce özelleştiren ve daha sonra rekabeti başlatan ülkelere göre maliyetleri daha hızlı düşüreceklerini vurgulamıştır.

www.igbook.info/digitaldivide

Kapasite geliştirme

İnternet yönetişiminin etkinliği ve meşruiyeti, ulusların, kuruluşların ve bireylerin İnternet yönetişimi politika süreçlerine tam olarak katılma kapasitelerine bağlıdır. Bunların kapasiteleri, “sorunları tanımlamak ve çözmek, bilinçli seçimler yapmak, önceliklerini sıralamak, geleceklerini planlamak ve bunları sürdürmek için programlar ve projeler uygulamak” için onların yetenekleri demektir.²⁶

Kapasite geliştirme hakkında

Kapasite geliştirmenin önemi konusunda bir anlaşma olsa da, ne içerdiği hakkında çok az bir uzlaşma vardır. Dahası, kapasite geliştirme popüler bir konuşma kavramıdır. Diplomatik müzake-

relerde, kapasite geliştirme, müzakerelerin diğer yönleri hakkında küçük bir anlaşma olduğunda, asgari müşterek olarak kullanılır.

Tipik olarak, kapasite geliştirme eğitim olarak anlaşılmaktadır. Terimin bu yorumu, eğitimin gelişmiş ülkeler tarafından gelişmekte olan ülkelere sağlanan teknik yardım programlarının merkezinde yer aldığı 1950'lere ve 1960'lara kadar uzanır. Daha sonra, 1970'lerde teknik işbirliği kavramı, beceri ve bilginin basit transferinin ötesinde, ulusal politikalar ve öncelikler içerisinde ele alınmaya doğru ilerlemiştir. Daha yakın bir zamanda (1990'larda), kapasite geliştirme gelişmekte olan ülkelerdeki içsel kapasiteleri güçlendirmeye ve sağlamlaştırmaya odaklanmaya başlamıştır.

Kapasite geliştirme mi, kapasite kurma mı

Kapasite geliştirme ve kapasite kurma, kalkınma tartışmalarında sıklıkla duyulan iki terimdir. Birincisi, tüm ülkelerde mevcut olan içsel kapasiteler ve becerilerin geliştirilmesine atıfta bulunurken, ikincisi sıfırdan başlayarak ve daha önce var olmayan bir şeyi inşa etme sürecine atıfta bulunmak için kullanılır. Kapasite geliştirme mevcut kalkınma terminolojisinde daha yaygın olarak kullanılmaktadır.

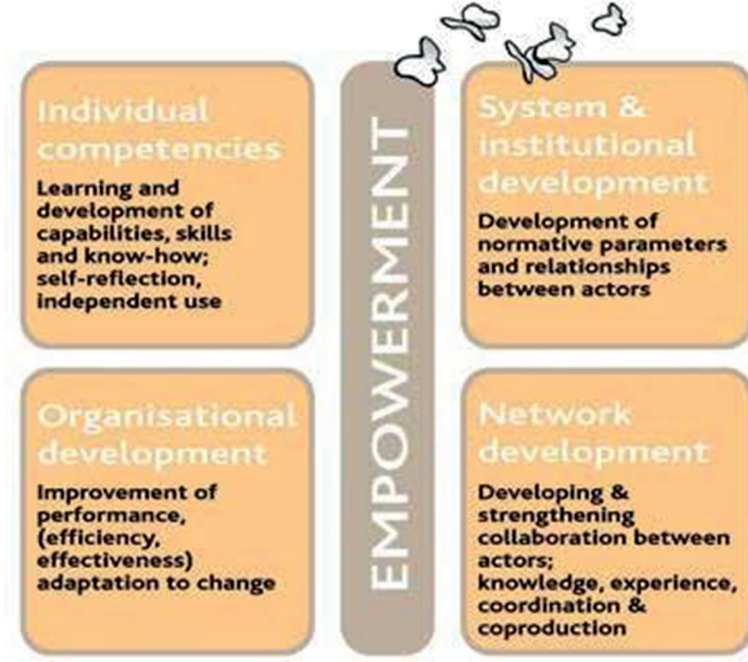
Kapasite geliştirme, kapasite türleri ve geliştirildikleri seviyelere referansla tanımlanabilir.

Kapasite türleri:

- Mühendislik bilgisi gibi teknik ve uzmanlık bilgisini ve bunun nasıl yapıldığını bilen (know how) katı kapasiteler.
- Genellikle iki alt gruba ayrılan yumuşak kapasiteler:
- Kültürlerarası iletişim, liderlik, örgüt kültürü ve değerleri, problem çözme becerileri gibi operasyonel kapasiteler.
- Analiz etme ve uyarlama yeteneği, hazırlık ve yönetimi değiştirme, güven gibi uyarlanabilir kapasiteler.

Sert kapasiteler genellikle teknik ve görünür olarak adlandırılır, yumuşak kapasiteler ise rasyonel ve görünmez olarak tanımlanır.

Kapasitelerin geliştirildiği ve ihtiyaç duyulduğu çeşitli seviyeler, kapasite geliştirme kelebeği ile görselleştirilir (İsviçre Kalkınma ve İşbirliği Ajansı tarafından kullanılan metodolojiye dayanan Şekil 22).²⁷



Şekil 22. Kapasite geliştirme kelebeği

İnternet yönetiřimi ve dijital politikada kapasite geliřtirme

Kapasite geliřtirme ihtiyaçı, WSIS'in 2003-2005 yılları arasında geliřmekte olan ölkeler için öncelikli olarak kapasite geliřtirmeyi vurgulayan belgelerden bu yana, İnternet yönetiminde temel bir özellik olmuřtur. Aynı řekilde, 2015 WSIS + 10 sonu belgesi de kapasite geliřtirmeye daha fazla yatırım yapılması çağrısında bulunmaktadır.

İnternet yönetiřiminin yeni doęası göz önüne alındığında, asıl odak nokta bireysel eęitim ve politika konuları olmuřtur.

ITU, DiploFoundation ve Cenevre İnternet Platformu (GIP)²⁸, APC, İnternet Topluluęu ve ICANN dahil olmak üzere birçok kuruluřta kapasite geliřtirme programları hazırlanmıřtır. İnternet yönetimindeki çeřitli bölgesel yaz okulları da, özellikle geliřmekte olan ölkeler için kapasitenin güçlendirilmesine katkıda bulunmaktadır. Mevcut programların çoęu telekomünikasyon altyapısı, teknik standartlar, siber güvenlik, spam, BİT düzenlemesi, ifade özgürlüęü, e-ticaret, iř hukuku, eriřim ve dijital uçurumun üstesinden gelmeye odaklanmaktadır.

İnternet yönetimi ve dijital politika alanında yüzlerce kiři eęitilmiřtir. Daha olgun bir safhaya geiř, politika süreçlerine sürekli katılımın saęlanması ile organizasyonel geliřime daha güçlü bir odaklanma gerektirecektir. Bu, geliřmekte olan ölkelerde hükümetlerin, sivil toplum örgütlerinin, iřveren kuruluřlarının ve akademi'nin örgütsel kapasitelerinin geliřtirilmesini içerir.

Örgütsel ve sistem düzeyinde kapasite geliştirme, siber güvenlik gibi sorunlarla başa çıkmada özellikle önem kazanmaktadır.

Genel olarak kapasite geliştirme araştırması ve İnternet yönetişimi alanındaki deneyim, aşağıdaki olaylara yol açmaktadır:

- İnternet küresel bir imkan olmakla birlikte, İnternet politikası genellikle çok yereldir. İçeriğe yönelik kültürel duyarlılık, mahremiyet korumanın önemi gibi yerel kültürel ve sosyal özellikler ile şekillenir. Bu nedenle kapasite geliştirme, kapasite geliştirme programları ve faaliyetlerinin geliştirilmesi ve uygulanmasında yerel politik, sosyal, kültürel ve diğer özel koşulları göz önünde bulundurarak yerel dinamikleri takip etmelidir.
- Kapasite geliştirme aciliyeti, politika süreçlerinin bir parçası olarak tam zamanında öğrenmeyi sağlayarak giderilebilir. Bu yaklaşımın bazı unsurları DiploFoundation ve GIP tarafından, diplomatlar için tam zamanında eğitim programlarında, ayrıca ICANN tarafından, Burs Programında²⁹ ve İnternet Topluluğunda IGF Elçiler Programında³⁰ kullanılmaktadır.
- Dijital politika alanındaki artan kapasite ihtiyacı, daha sistematik bir düzeyde lisansüstü akademik öğretim programlarında internet yönetişimi ve ilgili konulardaki derslere yer verilerek sağlanmak zorundadır.
- Gerçek ve sürdürülebilir güçlendirme kapasite geliştirme kelebeğinde gösterildiği gibi bireysel, organizasyonel, sistem ve ağ seviyelerinde bütüncül kapasite geliştirme yoluyla sağlanabilir (Şekil 22).

www.igbook.info/capacitydevelopment

Son notlar

- 1 Bu tür iki çalışma için bkz. World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 29 Ekim 2016], and Alliance for Affordable Internet (2016) The 2015-2016 Affordability Report. <http://a4ai.org/affordability-report/report/2015/> [Erişim 5 Kasım 2016].
- 2 United Nations General Assembly (2002) Resolution A/56/183. World Summit on the Information Society. http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf [Erişim 27 Ekim 2016].
- 3 United Nations General Assembly (2000) Resolution A/55/L.2. United Nations Millennium Declaration. <http://www.un.org/millennium/declaration/ares552e.htm> [Erişim 27 Ekim 2016].
- 4 United Nations (no date) Millennium Development Goals. <http://www.un.org/millenniumgoals/> [Erişim 27 Ekim 2016].
- 5 United Nations General Assembly (2015) Resolution A/70/1. Transforming our world: the 2030 Agenda for Sustainable Development. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E [Erişim 27 Ekim 2016].
- 6 United Nations General Assembly (2015) Resolution A/70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf> [Erişim 27 Ekim 2016].
- 7 SDG'ler ve internet arasındaki bağlanılar hakkında daha fazla bilgi için bkz. GIP Digital Watch observatory (no date) Sustainable Development Goals and the Internet. Available at <http://digitalwatch.giplatform.org/processes/sustainable-development-goals> [Erişim 11 Ağustos 2016].
- 8 UNCTAD (no date) Information and Communication Technology for Development. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D.aspx [Erişim 27 Ekim 2016].
- 9 WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Development Goals. Geneva: International Telecommunications Union. https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf [Erişim 27 Ekim 2016].
- 10 WSIS Forum'unun 2015 ve 2016. Edisyonları için bkz. GIP Digital Watch observatory (no date) WSIS Forum 2015. <http://digitalwatch.giplatform.org/events/wsis-forum-2015> [Erişim 28 Ekim 2016]; and GIP Digital Watch observatory (no date) WSIS Forum 2016. <http://digitalwatch.giplatform.org/events/wsis-forum-2016> [Erişim 28 Ekim 2016].
- 11 World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 29 Ekim 2016].
- 12 OECD (2001) Understanding the Digital Divide. p. 5. <http://www.oecd.org/internet/ieconomy/1888451.pdf> [Erişim 27 Ekim 2016].
- 13 Internet World Stats (2016) Digital Divide Gap is Getting Smaller. <http://internet-worldstats.com/wp/digital-divide-gap-is-getting-smaller/> [Erişim 30 Ekim 2016].
- 14 WEF (2016) Global Information Technology Report. <https://www.weforum.org/reports/the-global-information-technology-report-2016> [Erişim 27 Ekim 2016].
- 15 European Union (2014) Universal Service. <https://ec.europa.eu/digital-single-market/universal-service> [Erişim 27 Ekim 2016].
- 16 European Commission (2016) Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code. <https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code>

[Erişim 28 Ekim 2016].

- 17 United Nations (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [Erişim 28 Ekim 2016]. For a discussion on the UN report, refer to Wagner A (2012) Is Internet access a human right? The Guardian, 11 January. <https://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right> [Erişim 28 Ekim 2016].
- 18 Internet Society (2012) Promoting the Use of Internet Exchange Points (IXPs): A Guide to Policy, Management and Technical Issues. <https://www.internetsociety.org/sites/default/files/Promoting%20the%20use%20of%20IXPs.pdf> [Erişim 5 Kasım 2016].
- 19 South Eastern European Dialogue on Internet Governance (2016) SEEDIG's contribution to the IGF 2016 Inter-sessional Programme on Policy Options for Connecting and Enabling the Next Billion – Phase II. <http://www.seedig.net/wp-content/uploads/2016/09/SEEDIG-contribution-to-IGF-CENB-II.pdf> [Erişim 28 Ekim 2016].
- 20 Berkman Center for Internet & Society, Harvard Law School (2003) BOLD 2003: Development and the Internet, Part 4: Solutions in the Architecture. <http://cyber.law.harvard.edu/bold/devel03/modules/modIC.html> [Erişim 28 Ekim 2016].
- 21 Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement. The ISP Column, January 2005, Internet Society, pp. 7–9. <http://www.potaroo.net/isp-col/2005-01/interconn.pdf> [Erişim 27 Ekim 2016].
- 22 The ITU-D Recommendation D.50, as well as its supplements, are <http://www.itu.int/rec/T-REC-D.50/e> [Erişim 11 Ağustos 2016].
- 23 United Nations (2015) Addis Ababa Action Agenda of the Third International Conference on Financing for Development. <http://www.un.org/esa/ffd/publications/aaaa-outcome.html> [Erişim 28 Ekim 2016].
- 24 World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 29 Ekim 2016].
- 25 Infocomm Development Authority of Singapore (no date) NEU PC Plus Programme. <https://www.imda.gov.sg/community/consumer-education/digital-inclusion/neu-pc-plus-programme> [Erişim 15 Ağustos 2016].
- 26 Swiss Agency for Development and Cooperation (2006) Glossary Knowledge Management and Capacity Development. https://www.eda.admin.ch/dam/deza/en/documents/publikationen/glossar/157990-glossar-wissensmanagement_EN.pdf [Erişim 5 Kasım 2016].
- 27 Swiss Agency for Development and Cooperation (2006) Capacity Development in SDC. https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-sdc_EN.pdf [Erişim 5 Kasım 2016].
- 28 Diplo'nun kapasite geliştirme faaliyetleri İnternet Yönetişimi Kapasite İnşası Programı; İnternet yönetişimi üzerine online kurslar, siber güvenlik, ve Teknik altyapı; MA in İnternet Yönetişimi ile entegre Çağdaş Diploması gibi alanları kapsamaktadır. Son zamanlarda, GIP operatörü olarak, Diplo kalıcı misyonlar için tam zamanında şeklinde eğitim sağlamaktadır.
- 29 ICANN (no date) ICANN Meeting Fellowships. <https://www.icann.org/fellowship-program> [Erişim 7 Kasım 2016].
- 30 Internet Society (no date) IGF Ambassadors Programme. <http://www.internet-society.org/what-we-do/education-and-leadership-programmes/next-generation-leaders/igf-ambassadors-programme> [Erişim 7 Kasım 2016].

The background is a solid teal color. It features several large, semi-transparent geometric shapes: a large inverted triangle at the top left, a smaller inverted triangle at the top right, a circle with diagonal lines on the right side, and several large triangles at the bottom, some of which are semi-transparent and overlap each other.

Bölüm 7

Sosyokültürel sepet

SOSYOKÜLTÜREL SEPET

İnternet, modern toplumun sosyal ve kültürel dokusunu önemli ölçüde etkilemiştir. Sosyal hayatımızın İnternet'ten etkilenmeyen bir bölümünü tanımlamak zordur. İnternet yeni sosyal iletişim modellerini ortaya koymakta, dil engellerini ortadan kaldırmakta ve yeni etkili ifade biçimleri yaratmaktadır ki, bunlar onun etkilerinden sadece birkaçıdır. Günümüzde internet, teknolojik olduğu kadar sosyal bir fenomendir.

İçerik politikası

Başlıca sosyokültürel konulardan biri, genellikle (ulusal güvenlik ve ahlak ve kamu düzeninden politik olarak motive edilmiş sansür biçimlerine kadar çeşitli hususların dayattığı içerik kontrol önlemleri gibi) devlet politikaları, (içerik politikalarının ifade özgürlüğü ve iletişim hakkı gibi haklar gibi) insan hakları ve (içerik kontrol araçları gibi) teknolojiler gibi çeşitli bakış açılarından ele alınan içerik politikasıdır. Tartışmalar genellikle üç içerik grubuna odaklanır.

- Kontrolü konusunda küresel bir fikir birliği olan içerik. Buraya çocukların cinsel istismarı ile ilgili içerik, soykırımın gerekçesi ve terör eylemlerinin teşviki veya organizasyonu dahildir.
- Belirli ülkeler, bölgeler veya etnik gruplar için kendi dini ve kültürel değerleri nedeniyle hassas olan içerik. Küreselleşmiş çevrimiçi iletişim birçok toplumda yerel, kültürel ve dini değerler için zorluklar yaratır. Örneğin, Orta Doğu ve Asya ülkelerinde çoğu içeriğin kontrolü resmi olarak belirli kültürel değerlerin korunması ile haklı görülmektedir. Bu genellikle pornografik ve kumar web sitelerine erişimin engellenmesi anlamına gelir.
- Genellikle siyasi muhalifleri susturmak ve genellikle ulusal güvenlik ve istikrarı korumak iddiasıyla internette siyasi sansür.¹

İçerik politikası nasıl yürütülür?

İçerik politikası için alakart menü, farklı kombinasyonlarda kullanılan aşağıdaki yasal ve teknik seçenekleri içerir.

Hükümetin içeriği filtrelemesi

İçeriğe erişimi filtreleyen hükümetler genellikle vatandaşların erişimi için engellenen bir İnternet İnternet Dizini oluşturur. Teknik olarak konuşursak, filtreleme temel olarak yönlendirici tabanlı IP engelleme, proxy sunucuları ve DNS yönlendirmesini kullanır. İçeriğin filtrelenebilmesi birçok ülkede gerçekleşir. Genellikle Çin, Suudi Arabistan ve Singapur gibi bu uygulamalarla ilişkili ülkelere ek olarak, diğer ülkeler de filtreleme önlemlerini giderek daha fazla uygulamaktadır.²

Özel derecelendirme ve filtreleme sistemleri

Çeşitli ulusal engellerin (filtreleme sistemleri) geliştirilmesiyle İnternet'in parçalanma riskiyle karşı karşıya kalan W3C ve benzeri fikirli kurumlar, **kullanıcı tarafından kontrol edilen derecelendirme ve filtreleme sistemlerinin** uygulanmasını öneren proaktif adımlar atmışlardır. Bu sistemlerde, filtreleme mekanizmaları kişisel bilgisayarlardaki yazılımlarla veya İnternet erişimini kontrol eden sunucu seviyesinde uygulanabilir.

Bu olasılık, farklı ülkelerdeki ve kültürlerdeki kullanıcıların, İnternet'in ulusal veya kültürel olarak filtrelenmiş bloklara bölünmesine neden olabilecek ulusal müdahale ihtiyacını ortadan kaldırarak kendi filtreleme sistemlerini uygulamalarına izin verir. Hükümetlerin, filtreleme yapan devletlerin gerekli gördüğünü yapmak için vatandaşlarına güvenip güvenmeyecekleri meselesi ortada durmaktadır. Bunun, sistematik hükümetlerin sistematik filtrelemesi yerine, kullanıcı tarafından özelleştirilmiş ek bir yol olması muhtemeldir.

Belirli ülkelerdeki dini gerekçelerle hükümetin içerik kontrolü iyi bilinmektedir, ancak dini gerekçelerle filtreleme belirli kuruluşlar tarafından da uygulanabilir veya savunulabilir. Örneğin, 1998'de Scientology hareketi tarafından üyelerine bir yazılım paketinin dağıtıldığı bildirildi. Eleştirmenler "Scieno bakıcısı" yazılımını Scientology'yi eleştiren web sitelerine erişimi engellediğini iddia etmiştir.³ Diğer örnekler potansiyel olarak tüm popülasyonları etkileyebilir: örneğin, Avustralya Hristiyan Lobisi, Avustralya hükümetine karşı, Avustralya evlerinde ve mobil cihazlarda "yetişkin içeriğini" engelleyebilecek bir dışlama filtresi sistemi uygulamak için lobi yapmıştır.⁴

Coğrafi konuma göre içerik filtreleme

İçeriğe ilişkin diğer bir teknik çözüm, belirli web içeriğine erişimi kullanıcıların coğrafi veya ulusal kökenlerine göre filtreleyen **coğrafi konum yazılımıdır**. Yahoo! davası bu açıdan önemlidir çünkü Vint Cerf de olmak üzere dahil olan uzmanlar grubu, vakaların% 70-90'ında Yahoo!'nun Nazi hatırasını barındıran web sitelerinden birinin bölümlerine Fransa'dan erişilip erişilmediğini belirleyebildiğini göstermiştir.⁵ Bu değerlendirme, mahkemenin Yahoo!'ya Fransa'dan Nazi hatıralarına erişimi filtrelemesini isteyen nihayi bir karar çıkarmasına yardımcı olmuştur. 2000'deki Yahoo! davasından beri, sofistike coğrafi konum yazılımı geliştirilerek coğrafi konumun belirlenmesi hassasiyeti daha da artmıştır.

Arama motorları aracılığıyla içerik kontrolü

Son kullanıcı ve web içeriği arasındaki köprü genellikle bir arama motorudur. Bu nedenle, arama sonuçlarının filtrelenmesi, belirli içeriğe erişimi engelleyen bir araç olarak da kullanılır. Bu tür filtreleme genellikle hükümet politikalarına uymak için arama motorları tarafından uygulanır. Kayda değer bir örnek, Çin'deki Google'dır. 2006'da Google, arama motorunun yerel bir sürümünü (google.cn) başlatmaya karar vermiştir ve bu Çin hükümetinin sakıncalı olduğu düşünülen çevrimiçi içeriğin filtrelenmesine ilişkin politikalarına uymak amacıyla. Şirket, 2010 yılında Google.cn'de yapılan aramaları Hong Kong tabanlı sunucularına (filtrelemeden arındırılmış) yönlendirerek yaklaşımını değiştirmiştir. Bu, sonunda Google'ın Çin'deki faaliyet-

lerini kapatmasına yok açan gerginliğe yol açmıştır.⁶

Arama sonuçlarının filtrelmesi sadece hükümet alanından uygulanmamaktadır. Ticari çıkarlar da, az ya da çok açık ya da yaygın olarak meseleye karışabilir. Yorumcular, arama motorlarının kullanıcının bilgiye erişmesine aracılık etmedeki rolünü sorgulamaya ve kullanıcıların bilgi ve tercihlerini etkileme güçleri hakkında uyardıya başlamışlardır.⁷ Bu konu, internet şirketlerinin uygulamaları konusunda daha fazla şeffaflık isteyen hükümetlerin dikkatini giderek daha fazla çekmektedir. Örnek olarak, Ekim 2016'da yapılan bir konuşmada, Almanya Başbakanı Angela Merkel, İnternet şirketlerini arama motorlarında kullandıkları algoritmalar hakkında kamuya açık bilgiler vermeye çağırıştır. Merkel, böyle bir bilginin, kullanıcıların arama motorları aracılığıyla aldıkları bilgilerin onlara nasıl ve ne şekilde verildiğini daha iyi anlamalarını sağlayacaklarını söylemiştir. Şansölye konuyu “Saydam olmadıklarında algoritmalar algımızın bozulmasına neden olabilir, geniş bilgi birikimimizi daraltabilir” sözleriyle noktalamıştır.⁸

Web 2.0 zorluğu: kullanıcı tarafından oluşturulan içerik

Web 2.0 platformlarının (bloglar, forumlar, doküman paylaşım web siteleri ve sosyal medya) geliştirilmesiyle kullanıcı ve yaratıcı arasındaki fark bulanıklaştı. İnternet kullanıcıları, blog yazarları, videolar ve fotoğraf galerileri gibi büyük miktarda web içeriğinin yaratıcısı oldu. “Uygun olmayan” web sitelerini tanımlamak, filtrelemek ve etiketlemek karmaşık bir etkinlik haline gelmektedir. Metinler için otomatik filtreleme teknikleri gelişmiş olsa da, görsel içeriğin otomatik tanınması, filtrelmesi ve etiketlenmesi hala geliştirme aşamasındadır.

Bazen hükümetler tarafından kullanıcı tarafından oluşturulan ve uygunsuz olduğunu düşündüğü içerikle uğraşma girişimlerinde ele alınan bir yaklaşım, ülke genelinde YouTube ve Twitter gibi platformlara erişimi tamamen engellemektir. Bununla birlikte, bu maksimalist yaklaşım, eğitim materyali dahil olmak üzere, hedeflenmeyen içeriğin engellenmesine neden olmaktadır. Daha uç bir önlem, İnternet erişimini (Arap Baharı etkinliklerinde olduğu gibi⁹) sosyal ağ platformları üzerinden iletişimi engellemek için tamamen kesmektir.

Çevrimiçi olarak neyin yayınlanıp neyin yayınlanamayacağı tartışması giderek olgunlaştıkça, sosyal medya platformlarının kendileri, tolerans gereken veya izin verilmeyen içerikler arasındaki sınırı çizdikleri politikalarını resmileştirmeye başlamışlardır. Örneğin, Facebook'un Haklar ve Sorumluluklar Bildirimi şunları belirtmektedir: ‘Bu bildirim veya politikalarımızı ihlal ettiğine inanırsak Facebook'ta yayınladığınız herhangi bir içeriği veya bilgiyi kaldırabiliriz.’¹⁰ Ancak, bu tür politikaların uygulanması bazen meşru içeriği kaldıran platformlar gibi istenmeyen sonuçlara yol açabilir.

Otomatik içerik kontrolü

İnternet sosyal medya şirketleri için milyonlarca video, ses ve metin içeriği girişi arasındaki yasadışı içeriği belirlemek zordur. Bu zorluğun olası bir çözümü AI mekanizmalarının kullanımına bağlı olabilir. AI'nın bu alandaki potansiyelinin bir örneği, Google tarafından geliştirilen ve “nefret söylemi” ni ve diğer sözlü taciz ve taciz şekillerini çevrimiçi olarak tespit etmek amacıyla başlatılan **Konuşma Yapay Zekasıdır**.¹¹ Ekim 2016 itibarıyla, Google'ın güçlü veri teknolojisine

dayanan yazılım test aşamasındadır. Ancak, nefret söyleminin neyi oluşturduğuna dair kararlar almak için makine öğrenmesine güvenmek, bu tür sistemlerin nefret söylemi ile ironi ve alay arasında ayırım yapım yapamayacağı gibi birçok soruya yol açmaktadır.

İçerik kontrolündeki yasal ve politika araçları

Yazılı ve sözlü anlatım biçimindeki içerik her zaman kamu politikasının odağında olmuştur. Toplamlar, politik, güvenlik ve dini düşünceler temelinde neyin kabul edilebilir ve kabul edilemez içerik olduğuna karar verir. Politikalar ifade özgürlüğünü teşvik etmekten sansür empoze etmeye kadar uzanmaktadır. İnternet, bu hassas politika alanına bilginin ve içeriğin yayılmasını eskisinden çok daha kolay hale getirerek girmiştir. Bu nedenle, bir yandan, yoğun bir şekilde düzenlenmiş bir içerik politikası alanıyla ve diğer taraftan, geleneksel içerik politikasının İnternete uygulanabilirliği ile ilgili yasal bir boşlukla karakterize edilen paradoksal bir durumla karşı karşıya kalmaktayız.

Ulusal düzey

Çevrimiçi içerik politikası alanındaki yasal boşluk yasal belirsizlik sağlar. Bu alandaki ulusal düzenleme daha öngörülebilir bir yasal duruma getirebilir ve ifade özgürlüğü ve bilgi özgürlüğü gibi insan haklarının daha iyi korunmasını sağlayabilir. Ayrıca, yasal kurallar, hükümetlerin içerik politikasında sahip oldukları yüksek takdir yetkisini de azaltabilir. İş sektörü, özellikle de İSS’ler ve İnternet şirketleri, içerik politikası konularında karar vermek zorunda olduklarında belirsiz durumlardan kaçınarak da bundan yararlanabilirler.

Gerekçeli içerik kontrolü ve sansür arasındaki sınır çok belirsizdir ve bu nedenle bunun mevzuatta yer alması zorlaşırken, gerginlikler giderek mahkeme salonlarında çözülmektedir. Örneğin, Mayıs 2016’da platformlarında ırkçı ve homofobik içeriğe izin vermek için çeşitli sosyal medya kuruluşları açılmıştır.¹² Ayrıca, Kasım 2015’te Paris’te, 2014-2016’da İsrail’de gerçekleşen saldırıları takiben sosyal medya kuruluşları terörist propaganda yayılmasını kolaylaştırmanın yanı sıra teröristlerin iletişim kurması, üyelerini toplaması, saldırıları planlaması ve gerçekleştirmesi ve düşmanlarına korku salması¹³ için bir platform sağlamakla suçlanmıştır.¹⁴

Uluslararası girişimler

Terörist tehditlere ve teröristlerin faaliyetlerini yöneten ve ideolojilerini çevrimiçi olarak tanıttığı gelişmiş karmaşıklığa cevaben, çok taraflı forumlar zararlı içeriği sınırlamanın yollarını ele almaya başlamıştır. Örneğin, G7 liderleri “terörist gruplar tarafından İnternet ve sosyal medyayı terör amaçlarıyla sömüren tehdidinin önlenmesine yönelik çabaların arttırılmasını” kabul etmiştir.¹⁵ Ayrıca, BM Güvenlik Konseyi, Terörle Mücadele Komitesinden, teröristlerin İnternet’i anlatılarını tanıtmak ve başkalarını işe almak için İnternet’i kullanmasına karşı koymak için kılavuzlar ve iyi uygulamalar önermesini istemiştir.¹⁶ Daha açık bir şekilde, UNODC İnternet’in terörist amaçlarla kullanımı hakkında bir rapor yayınlamıştır.¹⁷

Terörist propagandaya ve kanunsuz aşırı materyallerin çevrimiçi dağıtımına karşı koyma konusunda daha fazla tartışma için Bölüm 3'e bakınız.

Bölgesel düzeyde, ana düzenleyici inisiyatifler, Avrupa ülkelerinde, ırkçılık karşıtı ve anti-Semizm de dahil olmak üzere, nefret söylemi alanında güçlü bir mevzuatla ortaya çıkmıştır. Avrupa bölgesel kurumları bu kuralları siber alana yaymaya çalışmıştır. İçerik sorununu ele alan birincil yasal araç, CoE 2003 [Siber Suç Sözleşmesine ek olarak](#), bilgisayar sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanlığı niteliğindeki eylemlerin cezai hale gelmesiyle ilgili [Ek Protokol](#)'dür.¹⁸ Daha pratik bir düzeyde, 2012'de AB, [İnterneti Çocuklar İçin Daha İyi Bir Yer Yapmak için Avrupa Stratejisini](#) kabul etti. Bu strateji kapsamında farkındalık yaratmayı hedefleyen, yasadışı içerikle mücadele eden, filtreleme ve içerik etiketlemesi getiren, çevrimiçi ortamda çocukların güvenliği konularında sivil toplumla birlikte çalışan ve teknolojinin çocuklar tarafından kullanımı hakkında bir veri tabanı yaratan çeşitli faaliyet ve programlar uygulanmıştır.¹⁹

AGİT de bu alanda etkindir. 2003'ten bu yana, ifade özgürlüğü ve İnternet'in (örneğin, ırkçı, yabancı düşmanlığı ve anti-Semitik propaganda ve şiddet içeren aşırılıkçılık ve terörizme yol açan radikalleşmeyle ilgili içerik gibi) olası yanlış kullanımlarına odaklanan özel bir konferans ve toplantı düzenlemiştir.

Meseleler

İçerik kontrolü ve ifade özgürlüğü

İçerik kontrolü, genellikle ifade özgürlüğünün olası bir kısıtlaması olarak görülür. Dünya çapında pek çok toplum, ifade özgürlüğünü destekleyerek istisnai ve kamusal olarak haklı içerik kontrolüne izin vererek bu hassas bölgeyi ele almaya çalışmaktadır. Bu, özellikle İlk Değişikliğin Nazilerle ilgili ve benzeri materyalleri yayınlama hakkı da dahil geniş bir ifade özgürlüğünü garanti ettiği ABD'de önemlidir.

İfade özgürlüğü, ABD'nin İnternetteki içerikle ilgili konulardaki uluslararası tartışmalardaki konumunu büyük ölçüde şekillendirmektedir. Örneğin, ABD [Siber Suç Sözleşmesini](#) imzalar-ken, bu sözleşmeye Ek Protokolü imzalayamaz, nefret söylemi ve içerik kontrolü ile ilgilenir. İfade özgürlüğü sorunu da Yahoo! davası çerçevesinde ele alınmıştır. Uluslararası girişimlerinde ABD, Birinci Değişiklikte öngörül-ğü gibi ifade özgürlüğünü tehlikeye atabilecek çizginin ötesine geçmeyecektir.

Yasadışı offline – yasadışı online

İnsan haklarında olduğu gibi, hakim görüş, içerik dünyası söz konusu olduğunda çevrimdışı dünyanın kurallarının İnternete uygulandığı yönündedir.

İnternet düzenlemesi için siber yaklaşımın argümanlarından biri, niceliğin (iletişim yoğunluğu, mesaj sayısı) niteliksel bir fark yarattığıdır. Bu görüşe göre, nefret söylemi sorunu, aleyhi-

ne herhangi bir düzenlemenin yürürlüğe girmediğinden değil, internet üzerinden paylaşım ve yayılmanın onu farklı bir hukuki sorun haline getirmesinden dolayıdır. Bu duruma giderek daha fazla kişi maruz kalmaktadır ve mevcut kuralları uygulamak zorlaşmaktadır. Bu nedenle, İnternet'in getirdiği farklılık, kuralların kendisiyle değil, temel olarak icra sorunları ile ilgilidir.

İçerik kontrolünün etkililiği

İnternet politikası üzerine yapılan tartışmalarda, temel argümanlardan biri, İnternet'in ademi merkezietçi doğasının sansürü atlayabileceği yönündedir. Devlete yönelik içerik kontrolüne sahip ülkelerde, teknik olarak yetenekli kullanıcılar bu kontrolün yollarını bulmuşlardır (örneğin, VPN'ler aracılığıyla filtrelenmiş içeriğe erişmek veya içeriği erişimin engellendiği yerden farklı bir yerde kullanılabilir yapmak). Ayrıca, uzmanlar filtreleme önlemlerinin teknik düzeyde olumsuz sonuçları olabileceği konusunda uarmaktadır. DNS düzeyinde engelleme, örneğin, DNSSEC'nin gelmesiyle çelişebilir ve İnternet'in parçalanmasına da yol açabilir.²⁰

Siber hukuktan internet düzenlemesine ilişkin daha fazla tartışma için Bölüm 4'e bakınız.

İçerik politikasından kim sorumlu olmalıdır?

İçerik kontrolü alanındaki ana oyuncular parlamentolar ve hükümetlerdir. Çoğu zaman, hangi içeriğin kontrol edilmesi gerektiğine ve nasıl uygulanacağına temel anayasal ilkeleri uygularlar. İnternet geçitleri olarak ISS'ler, genellikle devlet çözümlerine veya kendi düzenlemelerine göre (en azından çocuk pornografisi gibi geniş fikir birliği olan konularda) içerik filtrelemenin uygulanmasından sorumlu tutulmaktadır. Ebeveynler gibi bazı kullanıcı grupları, çocukları korumak için daha etkili bir içerik politikası oluşturma konusunda isteklidir. Çeşitli derecelendirme girişimleri, ebeveynlerin çocuklara uygun içeriği bulmalarına yardımcı olur. İnternet tarayıcı yazılımının yeni sürümleri genellikle birçok filtreleme seçeneği içerir.

İnternet şirketleri (Facebook, Google ve Twitter gibi) fiili içerik düzenleyicileri haline gelmektedir. Örneğin Google, unutulma hakkına bağlı olarak, arama sonuçlarından bağlantıların kaldırılması için yarım milyondan fazla talebe karar vermek zorunda kalmıştır.

İnternet şirketleri tarafından uygulanan içerikle ilgili çözüm mekanizmaları konusundaki tartışma için Bölüm 4'e bakınız.

Bu tür şirketler ayrıca, yasadışı çevrimiçi içerikle mücadele etmek amacıyla kamu makamları ile işbirliği çabalarında giderek daha fazla yer almaktadır. Bu eğilimin bir örneğiyle, Silikon Vadisi'ndeki teknoloji şirketleri, 2016 yılı boyunca ABD yetkilileriyle, özellikle de terörle ilgili içerikle ilgili olarak, çevrimiçi içerik kontrolü ile ilgili konularda işbirliği fırsatlarını tartışan birkaç toplantı yapmışlardır.²¹ AB'de, BT şirketleri, Avrupa'daki çevrimiçi nefret söyleminin

yayılması ile mücadele etmek için bir dizi taahhüt içeren yasadışı çevrimiçi nefret konuşması üzerine Davranış Kuralları konusunda Avrupa Komisyonu ile birlikte çalıştılar.²²

www.igbook.info/contentpolicy

Çevrimiçi eğitim

İnternet, eğitim için yeni olanaklar açmıştır. Çevrimiçi/e-öğrenme girişimleri, dünyada çapında katılımcılara derslerin verilmesi için İnterneti bir araç olarak kullanmaktadır. Aynı zamanda, e-öğrenme, üniversiteler gibi geleneksel ortamlarda yüz yüze öğrenmeyi desteklemek ve harmanlanmış öğrenmeye yol açmak için kullanılmaktadır. Geleneksel eğitimin yerini alamazsa da, e-öğrenme, özellikle zaman ve mekan kısıtlamaları sınıfa fiziksel olarak katılmayı engellediğinde yeni olanaklar sağlamaktadır. Son zamanlarda, çevrimiçi eğitim, kurumsal ve örgütsel değişikliklerin yanı sıra yükseköğretim reformu ile de ilişkilendirilmiştir.²³

Geleneksel olarak, eğitim ulusal kurumlar tarafından yönetilmektedir. Eğitim kurumlarının akreditasyonu, niteliklerin tanınması ve kalite güvencesi, tümü ulusal düzeyde yönetilmektedir. Ancak, sınır ötesi eğitim yeni yönetim rejimlerinin geliştirilmesini gerektirmektedir. Birçok uluslararası girişim, özellikle kalite güvencesi ve akademik derecelerin tanınması gibi alanlarda yönetim boşluğunu doldurmayı amaçlamaktadır.

Meseleler

Dünya Ticaret Örgütü (WTO) ve eğitim

DTÖ müzakerelerinde tartışmalı konulardan biri, devlet tarafından sağlanan hizmetler için serbest ticaret rejiminin istisnalarını belirten GATS'ın I. Maddesinin 3(b) ve 3(c) hükümlerinin yorumlanmasıdır. Başta ABD ve İngiltere tarafından desteklenen bir görüşe göre, bu istisnalar, yüksek öğrenimde serbest ticareti mümkün kılacak şekilde fiili olarak ele alınmalıdır. Bu görüş, ağırlıklı olarak, eğitimde küresel pazarda yer kazanmak için İngilizce konuşulan eğitim sektörünün çıkarları tarafından yönetilmektedir ve birçok ülkeden kayda değer bir itiraz gelmiştir.²⁴

Tartışmanın önemli yönlerinden biri, eğitimin bir meta mı yoksa bir kamu yararı olarak mı değerlendirileceği sorusuna odaklanmaktadır. Eğitimin bir mal olduğu düşünülürse, DTÖ'nin serbest ticaret kuralları bu alanda da uygulanacaktır. Kamu yararı yaklaşımı ise, kamu üniversitelerinin ulusal kültür için önem taşıyan kurumlar olarak özel statü aldığı mevcut eğitim modelini korumaktadır. Çevrimiçi eğitim, ticaretin serbestleştirilmesinden de etkilenebilir. Bazı yorumcular, eğitim politikasında olası bir "ticaret sızması" konusunda uyarılmaktadırlar.²⁵

Kalite güvencesi ve standartlaşma

Çevrimiçi öğrenme dağıtım sistemlerinin kullanılabilirliği ve bu pazara kolayca girilmesi, kalite güvencesi sorununu gündeme getirmiştir. Çevrimiçi teslimatın teknik yönlerine odaklanılması, malzemelerin ve öğretimin kalitesinin önemini göz ardı edebilir. Çeşitli olası zorluklar eğitim kalitesini tehlikeye atabilir. Bunlardan bir tanesi, çoğu zaman gerekli akademik ve eğitsel yete-

neklere fazlaca sahip olmayan ticari olarak yönlendirilen yeni eğitim kurumlarının kolay pazara girmesidir. Bir diğer kalite güvence sorunu da, mevcut basılı materyal temelli eğitim materyallerinin çevrimiçi bir ortama basit bir şekilde aktarılmasının, yeni ortamın spesifik eğitsel potansiyelinden yararlanamamasıdır. Bu yönüyle eğitim kurumları, çevrimiçi sunulan kursların tasarımını ve içeriğini değerlendirmek için standartlar ve kılavuzlar geliştirmeye başlamıştır.²⁶

Akademik derecelerin tanınması ve kredi transferi

Derecelerin tanınması, çevrimiçi öğrenme ortamında özellikle önem kazanmıştır. Çevrimiçi öğrenmeye konusunda asıl zorluk bölgesel ve küresel düzeyde derecelerin tanınmasıdır.

AB, *Avrupa Kredi Transfer ve Biriktirme Sistemi* (ECTS)²⁷ ile düzenleyici bir çerçeve geliştirmiştir. Asya-Pasifik bölgesi, öğrenci değişimi ve ilgili bir kredi sistemi için *Asya'daki Üniversite Hareketliliği ve Pasifik* (UMAP) programı²⁸ ile kendi bölgesel modelini sunmuştur.

Çevrimiçi öğrenmenin gelişen uygulamasında, geleneksel üniversitelerin geleneksel stratejilerini izleyerek kredilerin tanınması ve aktarılmasına yönelik bir eğilim bulunmaktadır.

Kitlesel Açık Çevrimiçi Kursların (MOOC) ilk yaygın kabulü ve bağımlılık döngüsü bu kursların çalışmasını sağlarken ve geleneksel ya da karma öğrenim sunan eğitim sistemlerinde sağlanan ile aynı ya da daha iyi kişisel etkileşim sağlamak için kaynaklar geliştirilirken bu kursların inovasyonu da evrilmektedir.

Çevrimiçi öğrenmenin standartlaşması

Çevrimiçi öğrenme gelişiminin erken evreleri, hızlı gelişim ve yüksek çeşitlilikte platform, içerik ve öğretim ile karakterize edilmiştir. Bununla birlikte, kredilerin veya diğer niteliklerin tanınmasını kolaylaştırmak ve asgari kaliteyi sağlamak için ortak standartlar geliştirme ihtiyacı vardır. Standardizasyonun çoğu özel ve profesyonel kuruluşlar tarafından yapılmaktadır.

BİT, öğretim ve gelişme

SDG'ler kapsayıcı ve eşit kalitede eğitim gerektiren ve herkes için yaşam boyu öğrenme fırsatları sağlayan iddialı bir hedef içermektedir (Hedef 4). Bu amaca ulaşmak, WSIS-SDGlerin matrisinde²⁹ gösterildiği gibi birkaç WSIS eylem çizgisine bağlanabilir. Bu, BİT'in eğitim için önemini vurgulamaktadır.

www.igbook.info/onlineeducation

Kültürel çeşitlilik

Kültürel çeşitlilik geniş bir kavramdır ve dil çeşitliliğini, ulusal kimlikleri, gelenekleri ve dinleri içerebilir. İnternet ve kültürel çeşitlilik arasındaki ilişki, çeşitli şekillerde iki mislidir. Bir yandan, İnternet, farklı kültürel geçmişlere sahip bireyler arasındaki alışverişi kolaylaştırması ve geniş enformasyon ve bilgi kaynaklarına erişimi sayesinde, kültürel çeşitliliğin küresel düzeyde

tanınmasına katkıda bulunabilir. İnternet ayrıca bireylere ulusal ve kültürel kimliklerini yansı-
tacak şekilde kendilerini ifade etmeleri için yeni olanaklar sunmaktadır. Öte yandan, WSIS’de
altı çizildiği gibi, kültürel çeşitlilik, kültürler arasında diyaloga ve saygıya dayanan kapsayıcı bir
bilgi toplumunun gelişimi için esastır.

Çevrimiçi ortamda, kültürel çeşitliliğin korunması, geliştirilmesi ve tanıtılması, diğerlerinin
yanı sıra, yerel içeriğin geliştirilmesini teşvik ederek sağlanabilir. Yerel içerik, ulusal kimlikleri ve
kültürel özellikleri yansıtmaya potansiyeline sahip olduğundan, çevrimiçi olarak daha fazla yerel
içeriğe sahip olmak, İnterneti daha çeşitli ve kapsayıcı bir alan haline getirmek ve bu özgün
kimlik ve özellikleri küresel düzeyde tanıtmak için ek fırsatlara dönüştürür.

Mevcut yerel içeriğin çevirisi, uyarlanması ve çevrimiçi dağıtımı ve yerli bilgiyi ve gelenekleri
dijital araçlarla yansıtan değişen enformasyonun korunması kültürel çeşitliliği teşvik eden diğer
yöntemlerdir. Dijital arşivler ayrıca yerel toplulukların güçlendirilmesine ve yerel mirasın bel-
gelenmesine ve korunmasına katkıda bulunabilir. Bu, özellikle teknolojik ihtiyaçları tamamen
yerelleştirilmiş yaklaşımları gerektirebilecek yalıtılmış veya göçebe topluluklarla ilgilidir. Yazı-
lının yerel dillerde üretilmesi ve dağıtılması aynı zamanda İnternetin benimsenme oranlarını
arttırma potansiyeline sahiptir.

www.igbook.info/culturaldiversity

Çok dillilik

İnternet ilk günlerinden beri İngilizce ağırlıklı bir dil ortamı olmuştur. Bazı istatistiklere göre,
web içeriğinin% 50’sinden biraz fazlası İngilizce’dir,³⁰ oysa dünya nüfusunun% 75’i İngilizce
bilmemektedir.³¹ Aynı zamanda, dünyanın en çok konuşulan dili olan Çince, tüm içeriğin yal-
nızca% 2’sini oluşturmaktadır. Birleşmiş Milletler Geniş Bant Komisyonu tarafından 2015 yı-
lında yayınlanan bir raporda, dünyadaki tahmini 7100 dilin sadece% 5’inin şu anda İnternette
temsil edildiği ortaya kondu. Ayrıca, Latin betiğinin kullanımının, özellikle etki alanı adlarını
okumak için birçok İnternet kullanıcısı için bir sorun olmaya devam ettiğini de not etmiştir.³²



Şekil 23. Çok dillilik

Bu durum birçok ülkenin çok dilliliği teşvik etmek ve kültürel çeşitliliği korumak için ortak harekete geçmesini sağlamıştır. Çokdilliliğin teşviki (Şekil 23) sadece kültürel bir mesele değil; İnternetin daha da geliştirilmesi ihtiyacı ile doğrudan ilgilidir. İnternet, toplumun daha geniş kesimlerinde kullanılacaksa, içeriğe daha fazla dilde erişilebilir olmalıdır.

İngilizce dili hala web’de aşırı temsil edilmekle birlikte, bu yavaş yavaş değişmeye başlamıştır. Gittikçe daha fazla insan çevrimiçi hale geldikçe, bazı diller giderek daha belirgin hale gelmektedir. Örneğin, 2011-2015 yılları arasında, Rusça dil içeriğinin % 41,5, İspanyolca dil içeriğinin % 15,5 ve Portekizce dil içeriğinin % 56 büyüdüğü bildirilmiştir.³³ Hintli ve Çinli kullanıcılarıdaki hızlı artış, benzer şekilde büyüyen bir Hintçe ve Çince çevrimiçi dil tabanına yol açabilir.

Meseleler

Latince olmayan alfabeler

Çok dilliliğin teşviki, çeşitli alfabe, senaryo ve karakterlerin kullanımını kolaylaştıran teknik standartlar gerektirir. Bilgisayarların çok dilli kullanımı ile ilgili ilk girişimlerden biri, farklı diller için karakter setlerinin kullanımını kolaylaştırmak için standartlar geliştiren, kar amacı gütmeyen bir kurum olan **Unicode Konsorsiyumu** tarafından gerçekleştirilmiştir. ICANN ve IETF, IDN TLD'leri (hem ccTLD'ler hem de gTLD'ler için) getirerek önemli bir adım atmıştır.³⁴

IDN'ler alan adlarının (Çince, Arapça, Kiril gibi) Latin alfabesi olmayan harflerle ve (Fransızca, Almanca, Macarca, Romence gibi) farklı aksan ve bağıntılarla Latin alfabesiyle yazılmış harflerle kullanılmasını kolaylaştırmıştır.

IDN'ler konusunda daha fazla tartışma için Bölüm 2'ye bakınız. IDNS.

IDN'ler, İnternet'i daha kapsayıcı hale getirmeye katkıda bulunur; çünkü etki alanı adlarına daha fazla dilde ve komut dosyasında erişme ve kaydolma olasılığı, İnternet'i kullanma konusunda daha fazla insanı güçlendirir. Alan adları sadece adresleme ve adlandırma ile ilgili değil aynı zamanda içerik ile de ilgilidir. Bu nedenle, yerel topluluklarla ilgilidir ve yerel içeriğin yerel dil ve alfabelerde kullanımını ve geliştirilmesini teşvik etme potansiyeline sahiptir.

Makine çevirisi

Makine çevirisini geliştirmek için birçok çaba gösterilmiştir. Tüm resmi faaliyetlerin tüm üye devletlerin dillerine çevrilmesi politikası göz önüne alındığında, AB, makine çevirisi alanındaki çeşitli geliştirme faaliyetlerini desteklemiştir. Her ne kadar büyük değişiklikler (örneğin, AI sistemlerinin kullanımı dahil) yapılmış olmasına rağmen, kısıtlamalar devam etmektedir.

İngilizce konuşamayan ülkelerde artan pazar fırsatları ile, İnternet şirketleri de platformlarında makine çevirisi araçları sunmaya başlamıştır. Örneğin, Facebook ve Instagram, kullanıcı tarafından oluşturulan içeriğin otomatik çevirilerini sağlamaktadır.

Uygun yönetim çerçeveleri

Çok dilliliğin teşviki uygun yönetim çerçeveleri gerektirir. Yönetişim rejimlerinin ilk unsuru, 2001 **Kültürel Çeşitlilik Evrensel Beyannamesi**⁴³⁵ gibi önemli belgelerin benimsenmesi de dahil olmak üzere, çok dilliliğe odaklanan birçok girişim başlatmış olan UNESCO gibi kuruluşlar tarafından sağlanmıştır. Çok dilliliğin bir başka önemli destekçisi de AB'dir, çünkü çok dilliliği temel politik ve çalışma ilkelerinden biri olarak görmektedir.³⁶

Sıradan kullanıcıların katkıda bulunmaları ve içerik geliştiricileri olmalarını sağlayan Web 2.0 araçlarının evrimi ve geniş kullanımı, çok çeşitli dillerde yerel içeriğin daha fazla kullanılabilir

olması için bir fırsat sunmaktadır. Bununla birlikte, çok dilliliğin teşviki için daha geniş bir çerçeve olmadan, bu fırsat daha büyük bir boşluğa neden olabilir, çünkü kullanıcılar daha geniş bir kitleye ulaşmak için ortak bir dil (genellikle İngilizce) kullanma baskısını hissetmektedir.

Anlamlı erişim

İnternetteki dilsel ve kültürel çeşitliliğe duyulan ihtiyaç, erişim ve gelişim ile ilgili önemli bir konudur. Yerel dillerde sağlanan yerel içeriğin kullanılabilirliği, insanlara çevrimiçi olmaları için bir teşvik sağlamaktadır. Aynı zamanda, insanların kendilerini çevrimiçi olarak kendi dillerinde ifade etmelerini ve içerik üretmelerini sağlamaktadır. Sonuç olarak, yerel içerik İnterneti daha kapsayıcı hale getirebilir ve dijital uçurumun kapanmasına yardımcı olabilir.

www.igbook.info/multilingualism

Küresel kamu yararı

İnterneti küresel ve kamu imkanı olarak tanımlamak ve korumak için çok sayıda çaba gösterilmiştir. Küresel kamu yararı, insanlığın ortak mirasından öte sıkça kullanılan bir kavramdır. Bu kavramlar birbirinin yerine kullanılabilir veya çok fazla örtüşebilir. Küresel bir kamu yararı olarak İnternet iki yaklaşımla tanımlanmaktadır: kullanımında rekabet olmayan ve kullanımından dışlanılamayan bir ekonomik yaklaşım ve ulusal egemenliğin ötesinde küresel bir altyapı olarak güvenlik yaklaşımı.

Ekonomik yaklaşım

İnternete küresel kamusal mal olarak bakan ekonomik yaklaşım iki özelliğe dayanmaktadır: (biri tarafından tüketilmesi diğerlerinden eksiltmediği için) rekabetin olmaması ve (bir kişiyi kullanmaktan men etmek mümkün olmadığı için) dışlanamazlık özelliği. Bu kriterleri takiben, Dünya Bankası³⁷ İnternet'in kusurlu bir kamu yararı olduğunu, çünkü kamu yararının özelliklerinden sadece birine sahip olduğunu savunuyor. Yani, İnternet bir yandan rekabete açık değildir, çünkü bir kişi tarafından kullanılması diğerlerinin ulaşılabilirliğini azaltmaz. İnternet, kullanımı tipik olarak bir biçimde veya başka şekilde ücrete tabi olduğu için diğer dışlanamazlık özelliğine sahip değildir.

Ancak, İnternet bütünsel bir varlık değildir. Bir çok yönü vardır. Bu nedenle, küresel kamu yararının durumu internete genel erişim, internetteki bilgi ve verilerin kullanımı, internet standartlarının kullanımı, çevrimiçi eğitime erişim gibi durumlar için uygulanabilir.

İnternetin temel özelliklerinden biri, kullanıcıların dünya çapında etkileşimi ile yeni bilgi ve bilgilerin üretilmesidir. Posta listeleri, sosyal ağlar ve bloglar aracılığıyla büyük miktarda bilgi üretilmiştir. **Creative Commons**³⁸ dışında, bu tür bilgilerin yasal kullanımını kolaylaştıracak bir mekanizma yoktur. Yasal bir belirsizlik içinde bırakıldığında, değişiklik ve ticarileştirme için uygun hale getirilir. Yaratıcılığın önemli bir temeli olan bu ortak bilgi havuzu tükenme riski altındadır. İnternet içeriği ne kadar fazla ticarileştirilirse, kendiliğinden değişimler o kadar az

olur. Bu, yaratıcı etkileşimin azalmasına neden olabilir.

Creative Commons gibi girişimlerle birleşen küresel kamu yararı kavramı, mevcut İnternet yaratıcı ortamını ve İnternet tarafından üretilen bilgileri gelecek nesiller için koruyacak çözümler sağlayabilir.

Güvenlik yaklaşımı

Güvenlik yaklaşımı, küresel bir kamu yararı olarak düşünülerek küresel İnternet altyapısını korumayı amaçlamaktadır. Bu yaklaşıma göre, küresel bir kamu yararı olarak İnternet, özellikle de ulusal hükümetlerin müdahalesinden korunmalıdır. Bu yaklaşımın bileşenleri genellikle açık deniz ve İnternet arasında bir benzetme yapar.

Analojiler konusunda daha fazla tartışma için Bölüm 1'e bakınız.

Genellikle, güvenlik yaklaşımı, DNS, yönlendirme ve İnternet protokollerini global kamu malları olarak kapsar.³⁹ İnternet standartları (özellikle TCP / IP) açık ve geneldir. İnternet yönetim rejiminin, küresel kamu malları olarak ana İnternet standartlarının korunmasını sağlaması gerektiği iddia edilmektedir.

Kamu ve özel sektör çıkarları arasında denge

İnternetin gelecekteki gelişiminin altında yatan zorluklardan biri, özel ve kamusal menfaatler arasında bir denge kurmaktır. Asıl soru, İnternet'in küresel bir kamu malı olarak gelişmesini sağlarken, özel sektöre uygun bir ticari ortamı nasıl sağlayacağıdır. Çoğu durumda, sıfır toplam bir oyun değil, bir kazan-kazan durumu söz konusudur. Birçok İnternet şirketi, gelir ve İnternetin yaratıcı gelişimini sağlayan iş modelleri geliştirmeye çalışmaktadır.

İnternet altyapısının işletilmesinde özel şirketler hakimdir. Ortaya çıkan zorluklardan biri, İnternet altyapısının özel mülkiyetinin, İnternet'in küresel bir kamu malı olarak statüsü ile uyumlaştırılmasıdır. Ulusal yasalar, tüm potansiyel kullanıcılara eşit haklar sağlamak ve taşınan içeriğe müdahale etmemek de dahil olmak üzere, belirli kamu gereksinimleri ile özel mülkiyetin kısıtlanma olasılığını sağlamaktadır.

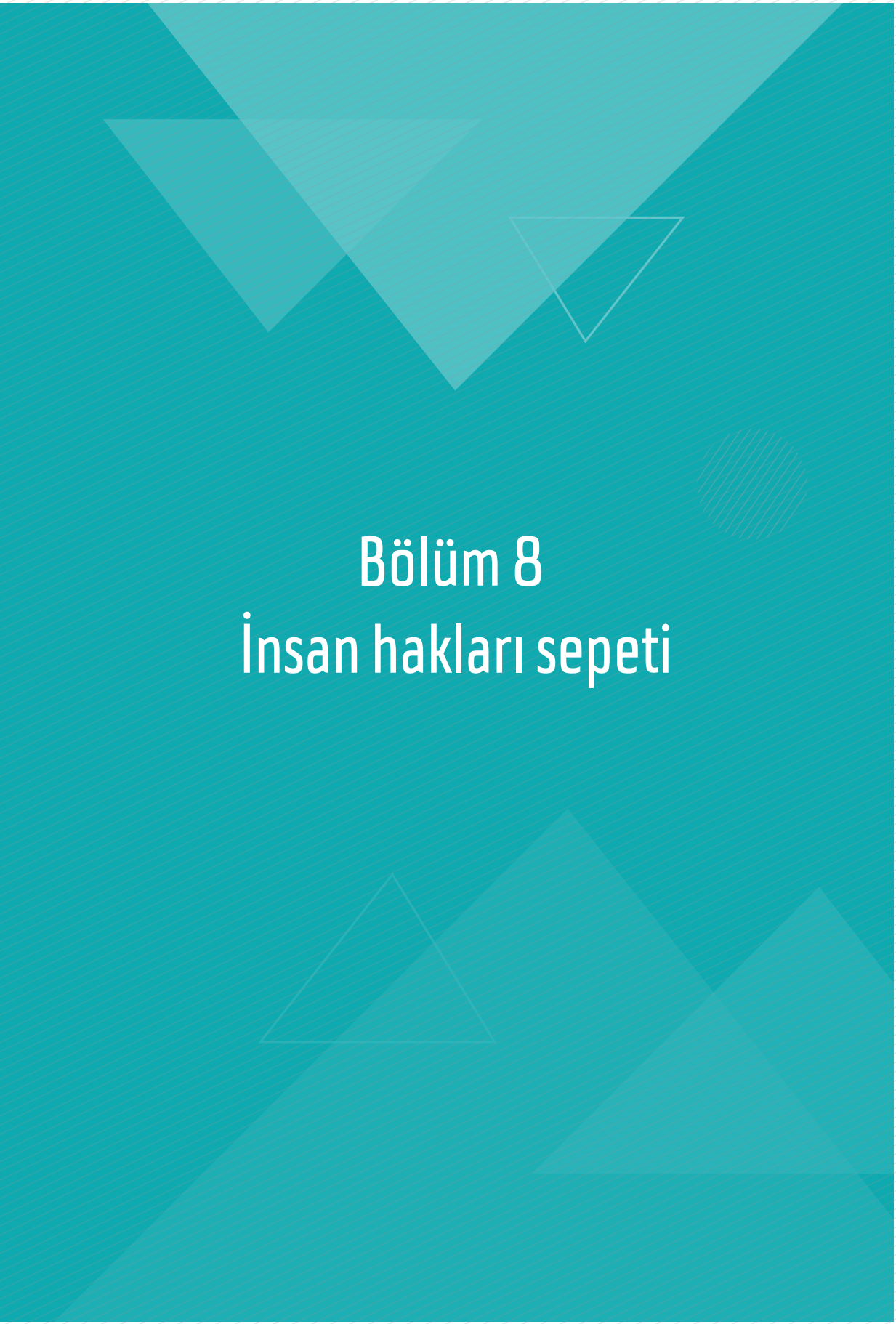
www.igbook.info/publicgoods

Son notlar

- 1 Freedom House, diğer konuların yanı sıra, dünyadaki hükümetlerin sansür politikaları uygulayıp uygulamamalarına bakan yıllık Net Özgürlük raporları yayınlamaktadır. Freedom House (no date) About Freedom on the Net. <https://freedomhouse.org/report-types/free-dom-net> [Erişim 2 Kasım 2016].
- 2 OpenNet Girişimi, dünyadaki ülkelerde gerçekleştirilen İnternet filtreleme ve gözetim uygulamaları hakkında veri toplar, analiz eder ve yayınlar. Ülke profilleri, bölgelere genel bakış ve web sitesinden erişilebilen etkileşimli haritalar sağlar. <https://opennet.net/> [Erişim 2 September 2016].
- 3 Operation Clambake (no date) Church of Scientology Censors Net Access for Members. <http://www.xenu.net/archive/events/censorship/> [Erişim 29 Ekim 2016].
- 4 Taylor J (2013) Australian Christian Lobby urges Coalition rethink on Internet filtering. ZDNet, 6 September. <http://www.zdnet.com/article/australian-christian-lobby-urges-coalition-rethink-on-internet-filtering/> [Erişim 29 Ekim 2016].
- 5 Her ne kadar Vint Cerf panele katıldıysa da, “çevrimiçi kapı kurmanın kusurlarına veya daha büyük etkilerine odaklanmadığını” söyleyerek nihai rapora itiraz etti. Kaynak: Guernsey L (2001) Welcome to the world wide web, passport, please? New York Times, 15 March 2001. Available at <http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm> [Erişim 29 Ekim 2016].
- 6 Waddell K (2016) Why Google Quit China – and Why It’s Heading Back. The Atlantic, 19 January. <http://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/> [Erişim 5 September 2016].
- 7 A good starting point to this debate is Mary Murphy’s blog post on DiploFoundation’s Internet Governance blog channel and the comments raised upon: Google...stop thinking for me! Available at <https://www.diplomacy.edu/blog/googlestop-thinking-me> [Erişim 29 Ekim 2016].
- 8 Connolly K (2016) Angela Merkel: Internet search engines are distorting perception. The Guardian, 27 Ekim. <https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception> [Erişim 30 Ekim 2016].
- 9 Crete-Nishihata M and York J (2011) Egypt’s Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. <https://opennet.net/blog/2011/01/egypt-s-internet-blackout-extreme-example-just-time-blocking> [Erişim 29 Ekim 2016].
- 10 Facebook (2015) Statement of Rights and Responsibilities. <https://www.facebook.com/terms> [Erişim 14 Temmuz 2016].
- 11 Greenberg A (2016) Inside Google’s Internet justice league and its AI-powered war on trolls. Wired, 9 September. <https://www.wired.com/2016/09/inside-googles-internet-justice-league-ai-powered-war-trolls/> [Erişim 30 Ekim 2016].
- 12 Chazan D (2016) Facebook, YouTube and Twitter sued for ‘failure to remove homophobic content’. The Telegraph, 15 May. <http://www.telegraph.co.uk/news/2016/05/15/facebook-youtube-and-twitter-sued-for-failure-to-remove-homophobic/> [Erişim 14 Temmuz 2016].
- 13 Williams D (2016) Relatives of Palestinian attack victims sue Facebook for \$1 billion in U.S. Reuters, 11 Temmuz. <http://www.reuters.com/article/us-israel-palestinians-facebook-idUSKCN0ZR1G0> [Erişim 14 Temmuz 2016].
- 14 BBC (2016) Twitter, Facebook and Google ‘aided Paris attacks’. 16 Haziran 2016. <http://www.bbc.com/news/technology-36548798> [Erişim 14 Temmuz 2016].

- 15 G7 (2016) G7 Action Plan on Countering Terrorism and Violent Extremism. [http:// www.mofa.go.jp/files/000160278.pdf](http://www.mofa.go.jp/files/000160278.pdf) [Erişim 18 Ağustos 2016].
- 16 UN News Centre (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 May. [http://www.un.org/apps/news/story. asp?NewsID=53909#V7VzGW5oQF](http://www.un.org/apps/news/story.asp?NewsID=53909#V7VzGW5oQF) [Erişim 18 Ağustos 2016].
- 17 UNODC (2012) The use of the Internet for terrorist purposes. Vienna: United Nations Office at Vienna. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Erişim 18 Ağustos 2016].
- 18 Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. <http://conventions.coe.int/Treaty/en/Treaties/html/189.htm> [Erişim 29 Ekim 2016].
- 19 European Commission (2015) From a Safer Internet to a Better Internet for Kids. <https://ec.europa.eu/digital-single-market/safer-internet-better-internet-kids> [Erişim 29 Oc- tober 2016].
- 20 İçerik filtreleme hakkında detaylar için bkz. ICANN Security and Sta- bility Advisory Committee (2012) SSAC Advisory on Impacts of Content Blocking via the Do- main Name System. [https:// www.icann.org/en/system/files/files/sac-056-en.pdf](https://www.icann.org/en/system/files/files/sac-056-en.pdf) [Erişim 5 September 2016], and Barnes A et al. (2016) Technical Considerations for Internet Services Blocking and Filtering (Internet Architecture Board RFC 7754). [https:// tools.ietf.org/html/rfc7754](https://tools.ietf.org/html/rfc7754) [Erişim 5 September 2016].
- 21 Yadron D and Wong JC (2016) Silicon Valley appears open to helping US spy agencies after terrorism summit. The Guardian, 8 January. [https://www.theguardian.com/tech- nology/2016/jan/08/techno-logy-executives-white-house-isis-terrorism-meeting-silicon-valley- facebook-apple-twitter-microsoft](https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft) [Erişim 18 Ağustos 2016].
- 22 European Commission (2016) European Commission and IT companies announce Code of Conduct on illegal online hate speech. [http://europa.eu/rapid/press-release_IP-16- 1937_en.htm](http://europa.eu/rapid/press-release_IP-16-1937_en.htm) [Erişim 18 Ağustos 2016].
- 23 Willcox K et al. (2016) Online Education: A Catalyst for Higher Education Reform. Massachusetts Institute of Technology. [https://professional.mit.edu/sites/default/files/MIT%20 Online%20Educa- tion%20Policy%20Initiative%20April%202016.pdf](https://professional.mit.edu/sites/default/files/MIT%20Online%20Education%20Policy%20Initiative%20April%202016.pdf) [Erişim 18 Ağustos 2016].
- 24 GATS'ın yüksek öğretime ilişkin yorumlarına ilişkin kapsamlı bilgi için bkz. Tilak J (2011) Trade in higher education: The role of the General Agreement on Trade in Services (GATS). Paris: UNESCO, International Institute for Educational Planning. [http:// unesdoc.unesco.org/ima- ges/0021/002149/214997e.pdf](http://unesdoc.unesco.org/images/0021/002149/214997e.pdf) [Erişim 29 Ekim 2016].
- 25 Knight J (2015) Trade creep: Implications of GATS for higher education policy. International Hig- her Education 28, pp. 5–7. [http://ejournals.bc.edu/ojs/index.php/ihe/article/ view/6658](http://ejournals.bc.edu/ojs/index.php/ihe/article/view/6658) [Erişim 29 Ekim 2016].
- 26 E - öğrenmeye ilişkin öneriler ve standartlarla ilgili örgüt ve çalışmaların örnek bir listesi için bkz., WBTIC (no date) Overview of E-learning Standards. [http:// wbtic.com/primer_standards.aspx](http://wbtic.com/primer_standards.aspx) [Eri- şim 29 Ekim 2016].
- 27 European Commission (no date) ECTS. [http://ec.europa.eu/education/tools/ects_ en.htm](http://ec.europa.eu/education/tools/ects_en.htm) [Erişim 29 Ekim 2016].
- 28 UMAP (no date) UMAP. <http://umap.org/about/> [Erişim 29 Ekim 2016].
- 29 WSIS Forum (2015) WSIS-SDG Matrix: Linking WSIS Action Lines with Sustainable Develop- ment Goals. Geneva: International Telecommunication Union. [https://www.itu.int/ net4/wsis/sdg/ Content/wsis-sdg_matrix_document.pdf](https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf) [Erişim 27 Ekim 2016].

- 30 W3Techs (2016) Usage of content languages for websites. https://w3techs.com/technologies/overview/content_language/all [Erişim 29 Ekim 2016].
- 31 British Academy Policy Centre (2011) Language Matters More and More. <http://www.ucml.ac.uk/sites/default/files/pages/160/Language%20Matters%20more%20and%20more.pdf> [Erişim 29 Şubat 2016].
- 32 The Broadband Commission for Digital Development (2015) The State of Broadband 2015: Broadband as a Foundation for Sustainable Development. <http://www.broadband-commission.org/Documents/reports/bb-annualreport2015.pdf> [Erişim 18 Ağustos 2016].
- 33 Wood J (2015) Top languages of the Internet, today and tomorrow. Unbabel, 10 Haziran. <https://unbabel.com/blog/top-languages-of-the-internet/> [Erişim 15 Temmuz 2016].
- 34 IDN programına genel bir bakış ve uygulanmasına ilişkin güncellemeler için bkz. ICANN (no date) Internationalized Domain Names. <https://www.icann.org/resources/pages/idn-2012-02-25-en> [Erişim 29 Ekim 2016].
- 35 UNESCO (2001) Universal Declaration on Cultural Diversity. http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html [Erişim 29 Ekim 2016].
- 36 European Commission (no date) Multilingualism. http://ec.europa.eu/languages/index_en.htm [Erişim 29 Ekim 2016].
- 37 World Bank (2016) World Development Report 2016: Digital Dividends. <http://www.worldbank.org/en/publication/wdr2016> [Erişim 29 Şubat 2016].
- 38 Creative Commons, dijital yaratıcılığı, paylaşımı ve yeniliği en üst düzeye çıkaran yasal ve teknik altyapıyı geliştiren, destekleyen ve bunlara eşlik eden kar amacı gütmeyen bir organizasyondur. <http://creativecommons.org/> [Erişim 29 Ekim 2016].
- 39 Broeders D (2015) The Public Core of the Internet. Amsterdam: Amsterdam University Press. http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf [Erişim 31 Ekim 2016].

The background is a solid teal color. It features several geometric shapes: a large inverted triangle at the top left, a smaller inverted triangle at the top right, a circle with diagonal lines on the right side, and several triangles of various sizes at the bottom.

Bölüm 8

İnsan hakları sepeti

İNSAN HAKLARI SEPETİ

İnternet ile ilgili temel insan hakları, mahremiyeti, İfade özgürlüğünü, bilgi alma, alma ve bilgi verme hakkını, kültürel, dilsel ve azınlık çeşitliliğini koruyan çeşitli hakları, ve eğitim hakkını içerir. Çocuk hakları ve gazetecilere ve basına verilen haklar gibi dijital politika alanında başka insan hakları da bulunmaktadır.

İnsan hakları (ifade özgürlüğü ve çevrimiçi mahremiyet gibi) genellikle açıkça ele alınsa da, aynı zamanda (erişim hakkı, ifade özgürlüğü, anonimlik gibi) ağ tarafsızlığına ilişkin konuları, (siber güvenlik ve koruma faaliyetlerini yürütürken insan haklarının gözletilmesi gibi) siber güvenlikle ilgili konuları, içerik kontrolü vb konuları da içermektedir.

Çevrim dışı insan haklarına karşı çevrimiçi insan hakları

UNGA ve UNHRC kararları ve CoE ve AB gibi bölgesel kuruluşlarda kabul edilen benzer belgeler, insanların çevrimdışı olarak kullandıkları aynı insan haklarının da çevrimiçi olarak korunması gerektiği ilkesini kesin olarak ortaya koymuştur. Gelişimci İletişim Derneği (APC), [İnternet Hakları Şartı](#)'nda, İnternet ile ilgili insan haklarının, [İHEB](#) ve diğer ilgili araçlara dayanan BM insan hakları sistemine dahil edildiğinin altını çizmektedir.¹

Çevrimdışı ve çevrimiçi haklar sorunu ilke olarak halledilmiş olsa da, çevrim içi düzenlemede çevrim dışı düzenlemenin uygulanması başka zorluklar doğurmaktadır. Çevrimiçi hakların özel bir yaklaşım gerektirdiğini söyleyenler, (iletişimin yoğunluğu, mesajların sayısı gibi) İnternet tarafından kolaylaştırılan çok miktarda iletişimin niteliksel bir fark yarattığını iddia etmektedir. Örneğin, nefret söylemi ile ilgili mesele, aleyhine düzenlemenin yapılıp yapılmadığı değil, internet üzerinden nefret söylemini paylaşma ve yayma kolaylığının onu farklı bir hukuki sorun haline getirmektedir. Çok sayıda çevrimiçi platform aracılığıyla daha fazla kişi nefret söylemine maruz kaldıkça, mevcut kuralları nefret söylemine karşı uygulamak giderek zorlaşmaktadır. Bu nedenle, mevcut kurallar uygun olsa da, İnternet uygulamasıyla ilgili zorluklar ortaya çıkmaktadır.

Teknoloji ve insan hakları

Teknik standartlar ve protokoller insan haklarının kullanılmasını etkiler. Altyapı sağlayıcıları, cihaz üreticileri ve standart kurumlarının tümü, İnternet'in teknik katmanında gömülü olan korumaların tanımlanmasında rol oynamaktadır. Şifreleme mekanizmaları ve 'İzlemeyin' gibi protokoller gizliliğin ve ifade özgürlüğünün korunmasını varsayılan değer olarak ayarlayabilir.

DNS düzeyinde, tartışmalar, örneğin, Şubat 2015'te ICANN tarafından onaylanan .sucks üst düzey alan adının serbest bırakılmasıyla ortaya çıkmıştır. Bazıları bu gelişmeyi ([marka] .sucks gibi ikinci seviye alan adı elde etmek için para ödenmesi gibi) zorbalık potansiyeli bakımından eleştirirlerken, diğerleri onu ifade özgürlüğünün kullanılması için bir alan olarak görmüşlerdir.² Bu ve benzeri kaygılar, teknik bir kuruluş olarak ICANN topluluğu içinde, insan haklarıyla ilgili yükümlülüklerin olup olmayacağı konusunda yoğun tartışmalara yol açmıştır. 2016 ICANN direktifleri, insan haklarını, ICANN'in kararlarına ve eylemlerine yol göstermesi gereken te-

mel değerler arasına dahil etmiştir: ICANN, “yasaların gerektirdiği şekilde uluslararası kabul görmüş insan haklarına” saygı duymaktadır. Bununla birlikte, bu temel değer, ICANN’ın (“İnternet’in benzersiz tanımlayıcı sistemlerinin istikrarlı ve güvenli bir şekilde çalışmasını sağlamak”) misyonu dışında veya yasada yer alan yükümlülüklerin ötesinde bir yükümlülük yaratmadığının altını çizilmektedir.³

İnternetle sağlanan ‘yeni’ insan hakları

Erişim hakkı

Estonya, 2000’de evrensel hizmet mevzuatı yoluyla İnternete erişme hakkını yasal olarak garanti eden ilk ülke oldu. Temmuz 2010’da Finlandiya vatandaşlarına 1Mbps genişbant bağlantısı için yasal bir hak verdi (hız Kasım 2015’ten 2 Mbps’e çıkarıldı). Diğer ülkeler vatandaşlarının İnternet’e erişim haklarını güvence altına almak için benzer adımlar attı.⁴ İnternete erişimin internette bir insan hakkı olarak tanınması konusunda dünyada farklı görüşler bulunmaktadır. Bazıları İnternete erişimin temiz suya, yiyeceğe ve diğer temel ihtiyaçlara erişim ile aynı olamayacağını savunmaktadır. Diğerleri, internete erişimin diğer temel insan haklarının yerine getirilmesini sağlamak için çok önemli olduğu için bunun yanlış bir ikilem olduğunu iddia etmektedir.

Ağ tarafsızlığı ve sıfır vergi erişim hakkını dünya kamuoyunun odağına erişim getirmiştir. Erişim hakkı söz konusu olduğunda ne tür bir İnternet erişimi kastediyoruz? Ücretsiz uygulamalarla sağlananlar gibi sınırlı sayıda web sitesine ve platforma erişimin İnternet erişimi olarak mı kabul edilmeli? Hindistan hükümetinin bu soruya yanıtı yanıt sıfır vergi ödenen hizmetleri yasakladığında olumsuz olmuştur. Diğer ülkeler bu sorunu tartışmaktadır. Aşağıdaki bakış açılardan hangisinin sıfır vergi tartışmasına hükmedeceği görülmeye devam edecektir: (erişim hakkı gibi) insan hakları mı, (ortaya çıkan iş modelleri gibi) ekonomik yaklaşım mı yoksa (yetersiz hizmet alan topluluklara yardım gibi) kalkınma yaklaşımı mı.

Unutulma hakkı

Unutulma hakkı ya da daha kesin bir şekilde endekslenmeme hakkı İspanya’da Google Şirketinin Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González’e karşı C - 131/12 dosya numaralı davası ile CJEU tarafından bir dönüm noktası olarak getirilmiştir. Dava, İspanya’daki La Vanguardia gazetesi tarafından Costeja’nın mülkiyeti için 1998’de ödenmemiş borçlardan dolayı yayınlanan bir açık artırma notu ile ilgiliydi. Bay Costeja, borçlarını yıllar önce ödemesine rağmen, gazete arşivleri dijitalleştirildikten sonra, adıyla Google’da yapılan aramalarda borçlu görünüyordu. İlk derece İspanya mahkemesi, gazete arşivinin bu bilgiyi artık göstermeyecek şekilde değiştirilmemesi gerektiğine karar verdi: medya özgürlüğü meselesi olarak kabul edildi. Ancak, İspanya Veri Koruma Kurumu (Agencia Española de Protección de Datos), Google’ın bu bilgilerin bağlantısını kaldırmasını istedi. Google, davayı CJEU’ya havale eden en yüksek ulusal mahkemenin (Audiencia Nacional) önünde itiraz etti.

13 Mayıs 2014’te, CJEU Google’a karşı hüküm tesis ederek davanın seyrini şu hale getirmiştir: Birincisi, ABD’de bulunan ve arama algoritmasının sahibi olan Google Şirketi’nin İspanyol

yan kuruluşunun arama motoru faaliyetlerinin ekonomik olarak “karlı olduğunu” belirleyerek yargı yetkisini 95/46 sayılı AB Veri Koruma Direktifi’nin uygulama kapsamına gireceği şekilde açıklamıştır. İkinci olarak, Google’ın “üçüncü taraflarca internette yayınlanan veya yer alan bilgileri bulma, otomatik olarak endeksleme, geçici olarak saklama ve son olarak belirli bir ter- cih sırasına göre İnternet kullanıcılarının erişimine açık hale getirme” faaliyetlerinden oluştuğu için Google’ın (verileri işleyen bir işletme olarak) bir veri denetleyicisi olduğunu belirlemiştir. Üçüncü olarak, Google’ın, Bir kişinin isminin üçüncü şahıslar tarafından yayınlanan ve bu ki- şiyle ilgili bilgileri içeren web sayfalarına, bu ismin veya bilginin önceden veya aynı anda bu web sayfalarından aynı anda silinmemesi durumunda ve hatta, bu sayfalarda kendi içinde yayınlan- ması yasal olduğu durumlarda, bir bazda yapılan arama sonrasında görüntülenen sonuçlar lis- tesinden çıkarılmasını sağlamak için Google’ın bir AB üye devletinin topraklarında denetleyici olarak Veri Koruma Direktifine uyması gerektiğine hükmedilmiştir.⁵ Mahkeme ayrıca, kamu çıkartı söz konusu olduğunda, veri denetleyicisinin belirli bir bağlantıya ulaşmaya devam edip etmeyeceğini değerlendirmesi gerektiğini kabul etmiştir.

Bu süreçte, CJEU, sunucu konumundan veya şirket merkezinden bağımsız olarak, kullanıcının konumuna göre verilerin işlenmesine dayanan yeni bir yaklaşım getirmiştir.⁶ CJEU kararını takip eden aylarda, Paris Tribunal de Grande’nin talebiyle Avrupa’dan erişim sağlandığı takdirde Google’ı (google.it, google.fr gibi) AB ülkelerine ait alt alan adlarından elde edilen sonuçları endekslemeden çıkarmaya zorlayan daha keskin bir durum ortaya çıkmıştır.⁷

Ayrıca, (1996 Direktifi’nin yerine) **Genel Verileri Koruma Yönetmeliği**nin kabul edilmesiyle, AB mevzuatta unutulma hakkını muhafaza ederek bir adım daha ileri gitti.⁸ Mayıs 2018’den başlayarak uygulanacak olan Tüzük, “silme hakkı (unutulma hakkı)” ile ilgili olarak, bireyle- rin kişisel verilerinin çeşitli gerekçelerle sildirtme hakkına sahip olduğunu ve Kontrolörün bu tür verileri gereksiz bir gecikme olmadan silme yükümlülüğünde olduğunu ifade etmektedir. Ek olarak, eğer kontrolör kişisel verileri halka açıkladıysa, ilgili verileri işleyen kontrolörlerin, verilerin konuyla ilgili olanların silinmesini veya kopyalanmasını veya çoğaltılması konusunda ‘makul adımlar atması’ gerekmektedir.

Unutulma hakkının düzenlenmesi iki karşıt görüşe yol açmıştır: bazıları bunu gizlilik ve veri koruma hakkının artırılması olarak görmekte, bu sayede kullanıcıların toplanan ve internet şirketleri tarafından saklanan verilerin silinmesini isteyebilecekleri bir süreci tanımlamaktadır. Diğerleri, yasal hükümler, başkasının haklarını ihlal etmese bile içeriğin silinmesine izin verecek şekilde uygulanırsa, bunu ifade özgürlüğü için olası bir tehdit olarak görmektedir.⁹ Hangi yasal hükümlerin uygulanacağı ve ve bu iki görüşün hangisi geçerli olacağı sorusu ortada durmak- tadır.

www.igbook.info/hr

İnternet ve mevcut insan hakları

İfade özgürlüğü ve bilgi alma, alma ve bilgi verme hakkı

Çevrimiçi ifade özgürlüğü son birkaç yılda diplomatik gündemde üst sıralarda yer almıştır. Örneğin, UNHRC'nin ve CoE gibi bölgesel hükümetlerarası organların gündemindedir. İnternette ifade özgürlüğü, IGF de dahil olmak üzere birçok uluslararası konferansta ve süreçte tartışıldı.

En kapsamlı yaklaşımlardan biri, yıllık toplantılara ev sahipliği yapan ve İnternette ifade özgürlüğü konusunda araştırma ve farkındalık yaratma çalışmaları yapan (Kasım 2016 itibariyle 30 hükümetin katılımı olan) Çevrimiçi Özgürlük Koalisyonu tarafından sağlanmaktadır.

Çevrimiçi ifade özgürlüğü tartışması çekişmeli bir politika alanı olmuştur. Çevrimiçi ifade özgürlüğü Genellikle devletin içerik kontrolü, sansürü ve gözetimi üzerine tartışmalar bağlamında ortaya çıkan temel insan haklarından biridir. Ek olarak, ifade özgürlüğü sorunu, nefret söyleminin yayılması ve İnternet üzerinde aşırı görüşlerin yaygınlaştırılmasına yönelik bazı güncel yaklaşımlarla karmaşılaşmakta ve bu gibi durumlarda ifade özgürlüğünü sınırlandırmayı amaçlayan tedbirler hem lehte hem de aleyhte ortaya atılmaktadır.¹⁰ Bununla birlikte, ifade özgürlüğünü sosyal sorumluluk lehine sınırlandırma yönünde bir eğilim var gibi görünmektedir.¹¹

Çevrimiçi ifade özgürlüğü aynı zamanda şifreleme ve anonimlik, ağ tarafsızlığı ve IPR gibi İnternet yönetimi ile ilgili konuları da kapsar. Bu hususların bazıları, ifade özgürlüğü hakkının güçlü bir şekilde korunmayı hak ettiğini birçok kere vurgulayan BM Özel Raportörü tarafından kaleme alınan raporlarda incelenmiştir. İfade özgürlüğü, insan hakları ve internete erişim konularında daha geniş biçimde ortaya çıkmaktadır.

İfade özgürlüğü, İHEB (Madde 19) ve Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi (Madde 19) gibi küresel araçlar ve Avrupa İnsan Hakları Sözleşmesi (Madde 10) küresel ve Amerikan İnsan Hakları Sözleşmesi (Madde 13) gibi bölgesel belgelerde korunmaktadır.

İHEB'de, ifade özgürlüğü, ahlak, kamu düzeni ve genel refah uğruna devletin ifade özgürlüğünü sınırlama hakkı ile dengelenmektedir (Madde 29). Bu nedenle, 19. maddenin hem tartışması hem de uygulanması, iki ihtiyaç arasında uygun bir denge kurulması bağlamında görülmelidir.¹² Bu belirsiz durum, normların farklı yorumlamaları ve nihayetinde farklı uygulamalar için birçok imkan sunar. Gerçek dünyada 19. ve 29. maddeler arasındaki doğru dengeye ilişkin ihtilaf bu dengenin internette gerçekleştirme tartışmalarına yansımaktadır.

Çevrimiçi ifade özgürlüğünü ele almak için ana yönetim mekanizması UNHRC'nin İnternet'teki İfade Özgürlüğünün Korunması Kararıdır (2012).

İfade özgürlüğü, İnsan Hakları İzleme Örgütü, Uluslararası Af Örgütü ve Özgürlük Meclisi gibi sivil toplum örgütlerinin odak noktasıdır. Örneğin, Özgürlük Meclisi, dünyadaki örnek ülkelerde ortalama kullanıcıların yaşadığı İnternet özgürlüğü seviyesini değerlendirmektedir. Onun 2016'daki Ağ Özgürlüğü çalışması, dünya çapında İnternet özgürlüğünün art arda altı yıl boyunca azaldığını ve değerlendirilen 65 ülkenin yarısından fazlasının sansür ve belirli İnternet servislerinin kullanımına getirilen sosyal medya kullanıcılarının tutuklanması, geniş gözetim ve belirli durumlarda tüm İnternet erişiminin kapatılması gibi kısıtlamalar gibi eylemler nedeniyle olumsuz bir yörüngede olduğunu belirtmektedir.¹³

Mahremiyet ve veri koruması¹⁴

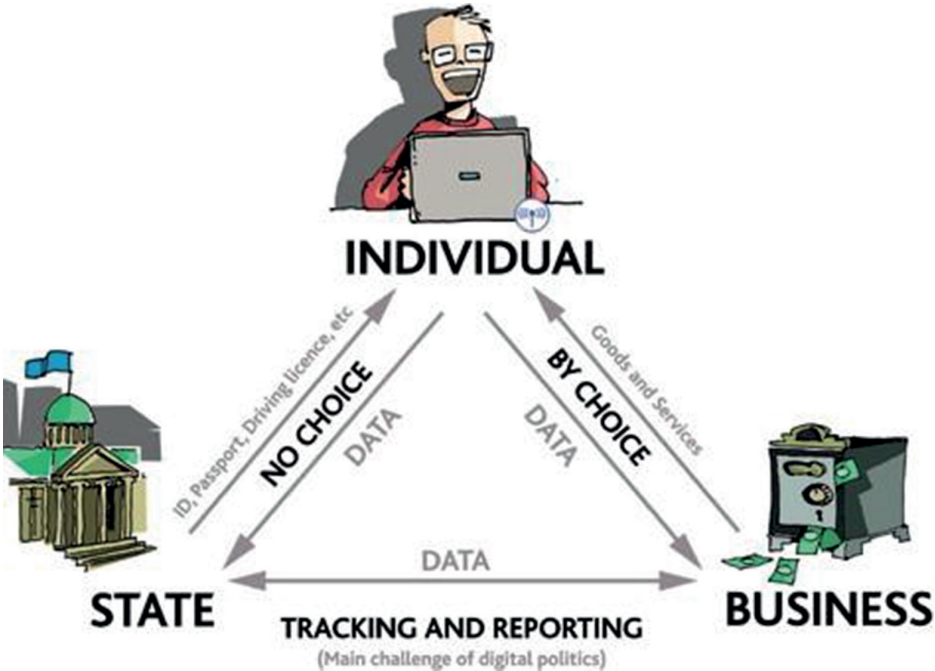
Gizlilik ve veri koruma, birçok İnternet yönetim sepetiyle ilgilidir: insan hakları, altyapı (veri yönetimi için standartlar geliştirme), güvenlik (ulusal güvenliğin korunması ve suça karşı mücadele için verilere erişim) ve ekonomi (verilerin bir iş modeli oluşturmak işlenmesi) sepeti gibi.

Gizlilik ve veri koruması birbiriyle ilişkili iki internet yönetişimi sorunudur. Gizlilik genellikle vatandaşların kendi kişisel bilgilerini kontrol etme ve ifşa edip etmeme konusunda karar verme hakkı olarak tanımlanır. Veri koruma, gizliliği sağlayan yasal bir mekanizmadır. Gizlilik, temel bir insan hakkıdır. **UDHR, Uluslararası Medeni ve Siyasi Haklar Sözleşmesi** ve diğer birçok uluslararası ve bölgesel insan hakları sözleşmesinde kabul edilmiştir.

Ulusal kültürler ve farklı yaşam biçimleri mahremiyet pratiğini etkiler. Mahremiyet özellikle Batı toplumlarında önemlidir, örneğin Almanlar mahremiyete yüksek önem vermektedir. Modern mahremiyet uygulamaları iletişim mahremiyetine (iletişimin gözetim altında olmamasına) ve bilgi gizliliğine (bireyler hakkında bilgilerin toplanmamasına) odaklanır. Geleneksel olarak, mahremiyet konusunda devlet gözetimi ile ilgili kaygılar vardır. Bununla birlikte, giderek artan bir şekilde, mahremiyet sorunları iş sektörünün ihlalleriyle de ilgilidir.

Meseleler

Temel gizlilik sorunları, Şekil 24'te gösterildiği gibi, bireyler, devletler ve işletmeler arasındaki üçgen kullanılarak analiz edilebilir.



Şekil 24. Dijital çağda mahremiyet

Mahremiyetin korunması: bireyler ve devletler

Bilgi her zaman devletlerin kendi bölgeleri ve toplulukları üzerinde otorite kullanmaları için önemli bir araç olmuştur. Hükümetler çok miktarda (doğum ve evlilik kayıtları, sosyal güvenlik numaraları, oy kaydı, sabıka kayıtları, vergi bilgileri, konut kayıtları, araç sahipliği gibi) kişisel bilgi toplar. Bir bireyin, aynı veri talebiyle karşı karşıya kalacağı başka bir ülkeye göç etmek yerine, devlete kişisel veri vermekten vazgeçmesi mümkün değildir. [Veri madenciliğinde](#)¹⁵ kullanılanlar gibi bilgi teknolojisi, karmaşık analizler yapmak, olağan ve sıradışı kalıpları ve tutarsızlıkları aramak için (vergilendirme, konut kayıtları, araç sahipliği gibi) birçok uzmanlık sisteminden verilerin toplanmasına ve ilişkilendirilmesine yardımcı olur (Şekil 25).

E-Devlet girişimlerinin temel zorluklarından biri, hükümet işlevlerinin modernizasyonu ile vatandaşların mahremiyet haklarının teminatı arasında, devletin meşru işlevlerini yerine getirmek ve kamu hizmetleri sağlamak için kesinlikle gerekli olan bilgilerin toplanmasını da içeren, uygun bir dengenin sağlanmasıdır. Bununla birlikte, son yıllarda hükümetlerin veri toplama konusundaki iştahının arttığına ve zorunlu tanımlama için (biyometrik veriler gibi) daha kişisel verilerin birleştirilmesine şahit olmaktadır.

ABD'deki 11 Eylül 2001'deki olayların ardından, [ABD Vatanseverlik Yasası](#),¹⁶ ve diğer ülkelerdeki karşılaştırılabilir yasalar, bilgilerin yasal olarak ele alınması için bir hükme dahil olmak üzere bilgi toplama yetkisini genişletmiştir. Kanıt toplamada yasal müdahale kavramı, CoE [Siber Suçlar Sözleşmesine](#) de dahildir (Madde 20 ve 21).

Mahremiyetin korunması: bireyler ve işletmeler

Mahremiyet üçgeninde de belirtildiği gibi (Şekil 24), ikinci ve giderek daha önemli bir ilişki bireyler ve iş sektörü arasındaki ilişkidir. Bireyler, bir banka hesabı açarken, bir uçuş veya otel rezervasyonu yaparken, çevrimiçi olarak kredi kartıyla ödeme yaparken, hatta İnternette gezinirken veya arama yaparken kişisel verilerini ifşa ederler: bu etkinliklerin her biri birden fazla veri izi bırakabilir.



Şekil 25. Veri madenciliği

Hem ticaretten müşteriye hem de şirketten ticarete kadar olan elektronik ticaretin başarısı ve sürdürülebilirliği, hem ticari mahremiyet politikalarına hem de müşterilerin gizli bilgilerini hırsızlık ve kötüye kullanımdan korumak için oluşturdukları güvenlik önlemlerine güven duyulmasına bağlıdır. Facebook, Twitter gibi sosyal ağ platformlarının genişletilmesiyle, kişisel verilerin nihai olarak suistimali ile ilgili sadece bir sosyal ağ platformunun sahibi veya yöneticisi tarafından değil, aynı zamanda onu kullanan diğer kişiler tarafından da endişeler ortaya çıkmaktadır.¹⁷ Ayrıca, İnternet şirketleri sık sık gizlilik politikalarını değiştirmeye meyillidir ve kullanıcılara her zamanki “kabul et veya ayrıl” dışında bir seçenek bırakmazlar. Kullanıcılar gizlilik politikasını kabul eder veya hizmeti kullanmamayı seçer.¹⁸

Bilgi ekonomisinde, müşteriler hakkındaki veriler tercihleri ve satın alma profilleri dahil olmak üzere önemli bir pazar ürünü haline gelir. Facebook, Google ve Amazon gibi bazı şirketler için, müşterilerin tercihleri hakkındaki bilgiler iş modellerinin temel taşlarını oluşturur. Temel olarak, kullanıcıların para ödedikleri çevrimiçi davranışını gösteren tarayıcı çerezi, bir web formunun doldurulması veya ödeme yapma gibi çevrimiçi hizmetler “ücretsiz” kullanıcıların kişisel verilerini elde etmek için hale getirilmiştir. Kullanıcılar kendileri hakkında daha fazla bilgi açığa vurdukça, mahremiyet ihlalleri daha sık ve daha karmaşık hale gelir.¹⁹

Mahremiyetin korunması: devletler ve işletmeler

Mahremiyet üçgeninin üçüncü tarafı en az kamuya açık, belki de en önemli gizlilik sorunudur.

Hem devletler hem de işletmeler bireyler hakkında önemli miktarda veri toplar. Devletler, terörle mücadele ve suçla mücadele faaliyetlerini desteklemek için verilere erişim sağlamak üzere (Facebook, Google gibi) İnternet iş şirketlerine çok fazla baskı uygulamıştır. Örnek olarak, Kasım 2015'te Paris'teki terörist saldırılardan sonra Fransız hükümeti, internet endüstrisi tarafından sağlanan verilere büyük ölçüde güvenmiştir. Benzer şekilde, hükümetler internet endüstrisi tarafından kullanılan daha güçlü şifreleme konusunda endişe duymakta ve bu da İnternet trafiğinin izlenmesini zorlaştırmaktadır.

İş dünyası, devlet baskısına karşı direnmeye ve devlet yetkilileri tarafından verilere erişimi kısıtlamaya çalışmaktadır. Devlet yetkilileri işletme verilerine erişirse, bu İnternet kullanıcıları arasındaki güven düzeyini azaltabilir ve İnternet şirketlerinin iş modelini etkileyebilir. Devlet makamları ile iş sektörü arasındaki bu gerginlik, önümüzdeki dönemde küresel dijital politika-daki temel sorunlardan biri olmaya devam edecektir.

Mahremiyetin korunması: bireyler ve bireyler

Mahremiyet üçgeninde görünmeyen mahremiyetin korunmasının son yönü, mahremiyet için bireylerden gelen potansiyel risktir. Bugün, yeterli fonu olan herkes güçlü gözetim araçlarına sahip olabilir. Bir kamera ile donatılmış basit bir cep telefonu bile böyle bir araç olabilir. The Economist²⁰ teknolojinin “demokratik gözetimi” gerçekleştirdiğini ifade etmiştir. Röntgencilikten bankalardaki kart numaralarını kaydetmek ve ekonomik casusluk için kameraların sofistike kullanımına kadar birçok mahremiyet istilası örneği ortaya çıkmıştır.

Bu tür mahremiyet ihlallerinden korunmanın temel sorunu, çoğu mevzuatın devletten veya özel şirketlerden kaynaklanan mahremiyet risklerine odaklanmasıdır. Bu yeni gerçeklikle karşı karşıya kalan birkaç hükümet bazı adımlar atmıştır. ABD Kongresi, çıplak kişilerin fotoğraflarının izinsiz olarak çekilmesini yasaklayan **Video Röntgencilik Önleme Yasası**'nı çıkarmıştır.²¹ Almanya ve diğer birkaç ülke, bireysel gözetimi önlemeyi amaçlayan benzer mahremiyet yasalarını kabul etmiştir.

Uluslararası gizlilik ve veri koruma düzenlemeleri

Mahremiyet ve veri korumayla ilgili uluslararası uluslararası araçlardan biri, 1981 yılındaki **Kişisel Verilerin Otomatik İşlenmesi Konusunda Bireylerin Korunmasına İlişkin CoE Sözleşmesi**'dir.²² Bölgesel bir kuruluş (CoE) tarafından kabul edilmesine rağmen, Avrupa ülkesi olmayan devletlerin erişimine de açıktır. Sözleşme teknolojiden bağımsız olduğu için zaman testine dayanmıştır.

1995 AB Veri Koruma Direktifi,²³ AB'de kişisel verilerin işlenmesi için önemli bir yasal çerçeve oluşturdu ve sadece Avrupa'da değil, aynı zamanda küresel olarak da ulusal mevzuatın gelişimi üzerinde büyük bir etkiye sahip oldu. Yeni gelişmelerle başa çıkmak ve mevcut teknolojik ortamda etkin mahremiyetin korunmasını sağlamak için yapılan bir reform sürecinin ardından,

2016 yılında Mayıs 2018'den itibaren geçerli olacak yeni bir **Genel Veri Koruma Yönetmeliği** kabul edildi ve 1995 Direktifinin yerine geçti.²⁴

Mahremiyetin ve verilerin korunmasına ilişkin bağlayıcı olmayan bir diğer önemli belge, 1980'de güncellenen 1980'den itibaren OECD'nin **Kişisel Verilerin Gizlilik ve Sınır Aşan Akışlarına İlişkin Kılavuz İlkeleri**'dir.²⁵ Bu kılavuzlar ve OECD'nin daha sonraki çalışmaları, mahremiyet ve veri koruma ile ilgili uluslararası, bölgesel ve ulusal düzenlemelere ilham vermiştir. Bugün, neredeyse bütün OECD ülkeleri mahremiyet yasalarını çıkarmış ve bu yasaları uygulamak için otoriteleri yetkilendirmiştir.

OECD kılavuz ilkelerinin yaygın olarak kabul görmesine rağmen, özellikle Avrupa ile ABD arasında nasıl uygulandıkları konusunda farklılıklar vardır. Avrupa'da, kapsamlı bir veri koruma mevzuatı vardır; ABD'de, ekonominin her bir sektörü için finansal mahremiyet (**Graham - Leach - Bliley Yasası**), çocukların mahremiyeti (**Çocukların Çevrimiçi Mahremiyetini Koruma Yasası**) ve tıbbi mahremiyet (**Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası** kapsamında) ile ilgili mahremiyet düzenlemesi geliştirilmiştir.

Diğer bir önemli fark, Avrupa'da mahremiyet mevzuatının kamu makamları tarafından yürürlüğe konması, ABD'de ise uygulamanın temel olarak özel sektöre ve öz düzenlemeye dayanmasıdır. İşletmeler kendi mahremiyet politikalarını belirler ve diğer şirketler ve bireyler kendilerini bilgilendirmekten ve buna göre davranmaktan sorumludur. ABD yaklaşımının ana eleştirisi, bireylerin mahremiyet politikaları tarafından sunulan seçeneklerin öneminin nadiren farkında olmaları ve kendilerini bilgilendirmeden genel olarak kabul etmeleri nedeniyle, nispeten zayıf bir konuma yerleştirilmesidir.

ABD ve AB arasındaki Gizlilik Kalkanı

ABD ve AB'nin mahremiyetin korunmasına yönelik farklı yaklaşımları, temel olarak kişisel verilerin özel şirketler tarafından işlenmesiyle ilgili soruları gündeme getirmiştir. AB, vatandaşları hakkındaki verilerin veri koruma yönetmeliklerinde belirtilen kurallara göre korunmasını nasıl sağlayabilir? Bir şirketin ağı üzerinden AB'den ABD'ye aktarılan verileri işlerken AB kuralları mı ABD kuralları mı geçerlidir? AB, yasal çerçevede belirtilen aynı mahremiyet korumasını sağlayamayacak herhangi bir ülkeye veri transferini engellemekle tehdit etmiştir. Bu talep kaçınılmaz olarak, ABD'nin mahremiyet korumasına ilişkin öz düzenleme yaklaşımıyla çatışmaya neden olmuştur.

Bu derin fark, herhangi bir anlaşmanın yapılmasını zorlaştırmıştır. Dahası, ABD yasalarını AB veri koruma yasasına uyarlamak, ABD hukuk sisteminin birkaç önemli prensibini değiştirmeyi gerektireceğinden mümkün olamazdı. Çıkmazdaki bu durumun ortadan kalkması 1998'de ABD Büyükelçisi David L. Aaron'un bir 'Güvenli Liman' formülü önerdiği zaman olmuştur. Bu öneri, meselenin tamamını yeniden şekillendirmiş ve müzakerelerde kördüğümünden çıkmak için bir yol sağlamıştır.

Güvenli Liman, Atlantik Okyanusu üzerinden veri alışverişi için yasal bir çerçeve oluşturmuştur. Veriler ABD'de bulunan sunucularda bulunsan bile, AB vatandaşlarının verilerinin AB kurallarına göre korunmasını sağlamaya çalışmıştır. Anlaşma, AB düzenlemelerinin yasal bir "güvenli

liman” içindeki ABD şirketlerine uygulanmasına izin vermiştir. AB vatandaşlarının verilerini işleyen ABD şirketleri, AB’nin gizlilik koruması gerekliliklerini gözlemlemek için gönüllü olarak kaydolabilmektedir. Anlaşmaya tabi olduktan sonra, AB ile ABD arasında kararlaştırılan resmi uygulama mekanizmalarını gözlemlemek zorunda kalmışlardır. Güvenli Liman Çerçevesi kapsamında, 4400’den fazla şirket yasal olarak AB’den ABD’ye 15 yıl boyunca veri aktarmıştır.

Bununla birlikte, Ekim 2015’te, Avrupa Birliği Komisyonu’nun ABD’nin AB vatandaşlarının verilerini “esasen eşdeğerde” korumasını sağlayıp sağlamadığını uygun bir şekilde değerlendirmemiş olduğunu göz önünde bulundurarak Avrupa Komisyonu, Güvenli Liman Çerçevesini geçersiz kılmıştır.²⁶ Bu karar AB ve ABD diplomatları arasında yeni bir mekanizma için görüşmeleri tetiklemiştir. Bu görüşmeler Temmuz 2016’da Avusturya, Bulgaristan, Hırvatistan ve Slovenya olmak üzere dört ülkenin çekimser oyuna karşın AB üye ülkeleri tarafından onaylanan **Mahremiyet Kalkanı** ile sonuçlanmıştır. O aydan sonra Avrupa Komisyonu, AB - ABD Mahremiyet Kalkanı’nın yeterliliğini doğrulayan bir kararı resmen onaylamıştır.²⁷

Kalkan, ABD şirketlerine AB vatandaşlarının kişisel verilerini korumak için daha güçlü yükümlülükler getirmekte ve ABD hükümetinden yeni hükümleri daha sağlam bir şekilde uygulamasını ve uygulamalarını izlemesini gerektirmektedir. Ek olarak, Gizlilik Kalkanı da önemli bir endişe alanı sunan bir konuyu ele almaktadır: ABD hükümetinin AB vatandaşlarının kişisel verilerine erişimi. Kalkan, ABD’den bu tür bir erişimin uygun sınırlamalara, güvencelere ve gözetim mekanizmalarına tabi olacağına dair güvence vermiştir. ABD hükümeti, AB’deki veri koruma makamlarıyla işbirliği yapmanın yanı sıra, ABD hükümetinin kişisel verilere erişimle ilgili bireylerin şikayetlerini almak ve bunlara cevap vermek için bir Ombudsman mekanizması oluşturma taahhüdünde bulunmuştur.

www.igbook.info/privacy

Dijital dünyada çocuk hakları

İnternet, çocuklar için birçok fayda sağlar ve aynı zamanda birçok risk içerir. Emin ve güvenli bir çevrimiçi ortam geliştirirken bu tür faydaların teşvik edilmesi, çocukların risklere karşı korunması ve çocukların bilgiye erişme ve konuşma özgürlüğü de dahil olmak üzere dijital haklarına saygı duyulması arasında dikkatli bir denge kurulmasını gerektirir.

Çocukların internet kullanımının güvenliği konusunda daha fazla tartışma için 3. Bölüme bakınız.

Birleşmiş Milletler Çocuk Hakları Sözleşmesi (ÇHS),²⁸ çocuk haklarının temel taşı olarak kabul edilir. ÇHS, en yaygın olarak onaylanmış uluslararası insan hakları anlaşmalarından biridir: bugüne kadar, ABD’nin bazı istisnaları dışında her BM üyesi devlet ÇHS’yi onaylamıştır.

ÇHS ilk kez çocukların insan haklarına sahip kişiler olduğunu kabul etmiştir. Sözleşme dört temel ilkeye dayanmaktadır:

- Çocuklar ayrımcılıktan muaf olmalıdır.
- Politikalar çocukların çıkarlarına hizmet etmelidir.
- Çocukların potansiyellerini tam geliştirmelerine imkan verilmeli ve bu teşvik edilmelidir.
- Çocukların görüşleri ve bakış açıları önemlidir ve duyulmaları gerekir.

Ayrıca, ÇHS genel olarak tedarik (provision), koruma (protection) ve teşvik (promotion) veya katılım (participation) şeklinde '3 P' olarak da adlandırılan üç geniş alana göre çocukların haklarını ele almaktadır.

Zorluklar

Korumacı yaklaşımlar

Çocukların çevrimiçi korunması, çocukların teknolojiyi kullanmasının koruyucu yönüne odaklanma eğilimindedir. Aslında, birçok kişi İnternet ve teknolojinin çocuklar için riskleri arttırdığını ve dolayısıyla çocukların yalnızca risklerin hafifletilmesi durumunda faydalardan yararlanabileceğini iddia etmektedir. Bununla birlikte, yalnızca çevrimiçi risklere odaklanan politikalar, İnternet'in çocukları güçlendirme potansiyelini sınırlayabilir.

Çocukların ÇHS gibi yasal araçlarda yer alan haklarına dayanan hak temelli bir yaklaşım, dijital dünyanın çocuklara ve gençlere yönelik fırsatlarını risklerden koruyarak en üst düzeye çıkarmayı amaçlamaktadır. Bu yaklaşım, çocukların dijital hakları ile korunma ihtiyaçları arasında daha dikkatli bir denge kurduğu için, uzmanlar tarafından giderek daha fazla tercih edilmektedir.

CRC'nin çevrimiçi dünyaya uygulanabilirliği

1989 yılında oybirliğiyle kabul edilen ÇHS, İnternet'in kitlesel kabulünden önce formüle edilmiştir. ÇHS çevrimiçi dünyaya uygulanıyor mu ve nasıl uygulanıyor?

2012 UNHRC'nin *İnternet'te insan haklarının geliştirilmesi, korunması ve kullanılmasına ilişkin Kararı*,²⁹ mevcut insan haklarının çevrimiçi olarak geçerli olup olmadığı veya çevrimiçi ortam için yeni bir haklar grubunun gerekli olup olmadığı tartışmasını sona erdirmiştir. Uzmanlar, bunun önemli bir başarı olmasına rağmen, çocukların korunmasında özel koruma gerektiren daha büyük adımların gerekli olduğu konusunda hemfikirdirler.³⁰

Özellikle ÇHS, çevrimdışı çocuk hakları ilkeleri ve idealleri konusunda fikir birliğine dayalı bir klavuz ve aynı ilke ve ideallerin uygun şekilde geliştirilmiş olması kaydıyla çevrimiçi olarak da kullanılabileceğini önermektedir. Bu nedenle ÇHS'nin net bir kurallar dizisine çevrilmesi gerekmektedir.³¹

ÇHS, hükümetlerin çocukların çıkarlarına en uygun şekilde davranma görevini yerine getirirken, bir dizi politika ve önlemin formüle edilebileceği bir çıkış noktası da sağlamaktadır.

www.igbook.info/children

Engelli kişilerin hakları³²

Dünya Sağlık Örgütü'ne (WHO) göre, dünyada yaklaşık 1 milyar engelli insan yaşamaktadır.³³ Bu sayı nüfus yaşlanması, yeni hastalıkların ortaya çıkışı, kronik sağlık koşulları, silahlı çatışma ve şiddet, yoksulluk ve sağlıksız yaşam koşulları, engelliliğin nedenleri, önlenmesi ve tedavisi hakkında yeterli bilginin olmaması nedeniyle artmaktadır.³⁴

İnternet, engellilerin sosyal hayata dahil olması için yeni olanaklar sunmaktadır. Engellilere ilişkin teknolojik olanakları en üst düzeye çıkarmak için, gerekli İnternet yönetiřimi ve politika çerçevesini geliřtirmeye ihtiya vardır. Bu alandaki ana uluslararası araç, Birleřmiř Milletler tarafından 2006 yılında kabul edilen ve řu anda bunları uygulanabilir kılacak olan ulusal yasalara dahil olma sürecindeki **Engelli Haklarına İliřkin Sözleřme'dir (UNCRPD)**.³⁵

Engellilere iliřkin teknolojik çözümlere duyulan ihtiya konusundaki farkındalık **IGF Eriřilebilirlik ve Engellilik Dinamik Koalisyonu**,³⁶ **İnternet Toplumu Engellilik ve Özel İhtiyalar řubesi**, **Uluslararası İnternetteki Engellilik Kaynakları Merkezi** gibi engelli topluma öğreten ve destekleyen kuruluşların çalışmaları ile artmaktadır.

Engelliler için erişilebilirlik sıkıntıları, donanım, yazılım ve içerik kullanmak için gereken yetenekler ile engelli bir kişinin mevcut kaynakları ve yetenekleri arasındaki boşluktan kaynaklanmaktadır. Bu açığı daraltmak için politikalar iki yönde ilerlemektedir:

- Ekipman, yazılım ve çevrimii içeriğın tasarımı ve geliřtirilmesi gereksinimlerine erişilebilirlik standartlarını dahil etmek.
- Engellilerin işlevsel yeteneklerini artıran veya deėiřtiren, donanım ve yazılımdaki aksesuarların kullanılabilirliğini arttırmak.

İnternet yönetiřimi alanında ana odak noktası, çevrimii içerik ve uygulamalar ile engelli kişilerin erişimine ve kullanımına uygun olmalarıdır. Web erişilebilirliğinde uluslararası standartlar, W3C tarafından **Web Eriřilebilirlik Giriřimi** kapsamında geliřtirilmiřtir. Bu tür standartların varlığına raėmen, pek çok çevrimii uygulama hala farkındalık eksikliği veya algılanan karmařıklık ve yüksek maliyetler gibi çeřitli nedenlerden dolayı bunlara uymamaktadır.

www.igbook.info/disabilities

Cinsiyet ve çevrimii insan hakları

Kadınların çevrimii hakları, hem İnternete erişim (örneğin çevrimii şiddet) hem de erişim eksikliği (örneğin, bilgiye, eğitime, iş dünyasına ve siyasi faaliyetlere erişim söz konusu olduėunda fırsat kaybı) ile ilgili çok çeřitli konuları içerir.

Tarihsel olarak, kızlar ve kadınlar, eğitimde (BİT uzmanlıkları dahil), sağlık, sosyal refah, politik katılım ve adalet alanlarında ayrımcılık ve büyük eşitsizliklerle karşı karşıya kalmışlardır. Temel haklardan yararlanmada kadınlarla erkekler arasındaki bu eşitsizliklerin biroėu çevrimii olarak sürdürölmüřtür. Şiddet, gö, çatışma ve krizler de özel alanlarındaki ciddi engellerle kadınların refahını ve hem çevrimdışı hem de çevrimii potansiyellerini kullanma yeteneklerini etkilemektedir.

Kadınlar dünya nüfusunun yarısından fazlasını temsil ediyor, ancak teknolojinin aracılık ettiği süreçlere katılımları hala ilerlemenin gerekli olduğu bir alan olarak durmaktadır. Kadın haklarının çevrimiçi ortamda korunması, eğitim ve ekonomik fırsatlara erişme, görevde bulunma ve eşit ücret alma da dahil olmak üzere hakların kullanılmasında ayrımcılığın azaltılmasına ve önyargının azaltılmasına dikkat etmeye odaklanan daha geniş bir sosyokültürel ve profesyonel değişimin parçasıdır.

İnternete erişim son yirmi yılda artmış olsa da, cinsiyetçi kullanım biçimleri eşit olmayan fırsatlar yaratmakta ve dünyadaki kız ve kadınların güçlendirilmesinde önemli boşluklar yaratmaktadır. 2016 yılı ITU verileri, küresel İnternet kullanıcı cinsiyet farkının 2013 yılında % 11'den 2016'da % 12'ye çıktığını ve erişimin en çok ihtiyaç duyulduğu yerler olan LDC'lerde hala çok yüksek (% 31) olduğunu göstermektedir: Veriler ayrıca bölgesel cinsiyet farkının Afrika'daki en yüksek (% 23) ve Amerika'daki en düşük (% 2) olduğunu göstermektedir.³⁷

Bir Web Foundation çalışmasına göre, cep telefonlarına daha gelişmiş erişim bile kadınları çevrimiçi hale getirmek için veya "kadınların teknolojiyle güçlendirilmesi" için yeterli değildir. Çalışma, çoğu kadın ve erkeğin bir telefona sahip olmasına rağmen, kadınların yalnızca % 37'sinin (aynı topluluktaki erkeklerin yaklaşık yarısı) internete erişme ihtimalinin olduğunu ve kadınların % 30-50'sinin ekonomik veya politik fırsatlar için internet kullanım oranlarının düşük olduğunu göstermiştir. Ayrıca, erişimin içsel olarak eğitim seviyesine bağlı olduğunu ve eğitiminin değişim için harekete geçilmesi gereken bir diğer faktör olduğunu göstermiştir.³⁸

Güçlendirilmiş çevrimiçi katılımla birlikte kadınların kamusal ve politik hayata katılımı artmaktadır, ancak BİT'lerin faydalarından tam anlamıyla faydalanmak, kadınlara erişimde eşitsizlik ve teknoloji ile ilgili şiddet gibi bir dizi engelin ortadan kaldırılmasına bağlıdır. Çevrimiçi araçlarla yapılan şiddet eylemleri arasında siber taciz, gözetim ve mahremiyet ihlalleri, cinsel taciz ve resimler ve videolar dahil olmak üzere kişisel bilgilerin yetkisiz kullanımı ve manipülasyonu yer almaktadır. Yaygın bağlantı çağında, İnternet araçlarının işbirliği ile daha güvenli çevrimiçi alanlar yaratmak, kadınların insan haklarının ve kalkınmasının tam olarak gerçekleştirilmesinde ilk adım olarak daha keskin bir odak noktası haline gelmektedir.

BM Özel Raportörü'nün kadına yönelik şiddete, nedenlerine ve sonuçlarına ilişkin 2016 raporunda, kadınlara yönelik çevrimiçi şiddeti yeni bir meydan okuma olarak kaydetti. Raporda, 'bilgi ve iletişim teknolojisinin kullanımı kadınların ve kızların güçlendirilmesine katkıda bulunurken, kullanımının da çevrimiçi şiddet yarattığını' belirtilmiştir. Rapor devletler ve devlet dış aktörlerin 'ifade özgürlüğüne zarar vermeden ve Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 20. maddesine göre şiddet ve nefretin teşvik edilmesini yasaklayarak kadınlara ve kızlara karşı çevrimiçi şiddetle mücadele etmeye' çağırılmaktadır.³⁹

Kadın haklarının korunmasına yönelik başlıca uluslararası araçlar, 1952 [Kadın Siyasi Haklarına İlişkin Sözleşme](#) ve 1979 [Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşmesi](#)'dir (CEDAW). Hem BM Kadın birimi hem de UNHRC, kadın haklarının çeşitli boyutlarında aktif olarak çalışmaktadır. Bununla birlikte, mevcut kadın hakları kuruluşlarının çevrimiçi faaliyet alanlarını yaygınlaştırmak kolay olmamaktadır. APC ve Cinsiyet ve İnternet Yönetişimi

Konusunda IGF Dinamik Koalisyonu gibi gruplar, kadınların çevrimiçi haklarını savunmak için aktif olarak yer almaktadırlar.

Kadın hakları hareketi olgunlaştıkça, bunların aslında diğer toplumsal cinsiyet azınlıklarının haklarını da kapsayan daha geniş toplumsal cinsiyet hakları sorunlarının bir parçası olduğunu kabul etmeye yönelik bir adım atılmıştır. Kadınlar ve Lezbiyen, Eşcinsel, Biseksüel, Trans ve Eşcinsel (LGBTQ) topluluğu dahil olmak üzere diğer toplumsal cinsiyet azınlıklarına yönelik insan hakları meseleleri, bilgiye erişim, mesleki fırsatlar, küresel politika süreçleri ve insan hakları için kritik olan diğer haklar ve İnternet yönetişimi vesırasıyla incelenmeli ve ele alınmalıdır.

www.igbook.info/gender

Son notlar

- 1 APC İnternet Hakları Şartı, herkes için İnternet erişimi içerir; ifade ve örgütlenme özgürlüğü; bilgiye erişim; paylaşılan öğrenme ve yaratma - özgür ve açık kaynaklı yazılım ve teknoloji geliştirme; gizlilik, gözetim ve şifreleme; İnternetin yönetimi; hakların farkındalığı, korunması ve gerçekleştirilmesi. <http://www.apc.org/en/node/5677> [Erişim 20 Ekim 2016].
- 2 Solon O (2015) Why the .sucks domain doesn't have to suck. Bloomberg, 19 Ağustos. <https://www.bloomberg.com/news/articles/2015-08-19/why-the-sucks-domain-doesn-t-have-to-suck> [Erişim 7 March 2016].
- 3 ICANN (2016) Bylaws for Internet Corporation for Assigned Names and Numbers. <https://www.icann.org/resources/pages/governance/bylaws-en> [Erişim 7 Ekim 2016].
- 4 Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. <https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it> [Erişim 20 Ekim 2016].
- 5 CJEU (2014) Judgement of the Court in Case C-131/12: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL> [Erişim 20 Ekim 2016].
- 6 Radu R and Chenou JM (2015) Data control and digital regulatory space(s): towards a new European approach. Internet Policy Review 4(2). <http://policyreview.info/articles/analysis/data-control-and-digital-regulatory-spaces-towards-new-european-approach> [Erişim 20 Ekim 2016].
- 7 Bowcott O and Willsher K (2014) Google's French arm faces daily €1,000 fines over links to defamatory article. The Guardian, 13 Kasım. <https://www.theguardian.com/media/2014/nov/13/google-french-arm-fines-right-to-be-forgotten> [Erişim 20 Ekim 2016].
- 8 European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679> [Erişim 14 Temmuz 2016].
- 9 Unutulma hakkının sonuçları konusunda daha fazla detay için bkz. Keller D (2016) The new, worse 'right to be forgotten'. Politico, 27 January. <http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/> [Erişim 14 Temmuz 2016].
- 10 Aşırı görüşlerin ifadelerini kısıtlama nedenlerinin yanı sıra dış görünüşler de dahil olmak üzere daha geniş konuşma özgürlüğüne izin veren argümanlar hakkında genel bilgi için, Heinze E (2014) Nefret konuşma yasakları için on dokuz argümana - ve bunlara karşı argüman için bkz. <http://freespeechdebate.com/en/discuss/nineteen-arguments-for-hate-speech-bans-and-against-them/> [Erişim 12 Ağustos 2016].
- 11 Poushter J (2015) 40% of millennials OK with limiting speech offensive to minorities. Available at <http://www.pewresearch.org/fact-tank/2015/11/20/40-of-millennials-ok-with-limiting-speech-offensive-to-minorities/> [Erişim 12 Ağustos 2016].
- 12 United Nations (1948) The Universal Declaration of Human Rights. <http://www.un.org/en/documents/udhr/> [Erişim 20 Ekim 2016].
- 13 Freedom House (2016) Freedom on the Net 2016. <https://freedomhouse.org/report/freedom-net/freedom-net-2016> [Erişim 16 Kasım 2016].
- 14 Electronic Frontier Foundation (EFF) Uluslararası Haklar Direktörü Katitza Rodriguez tarafından değerli yorumlar ve girdiler sağlanmıştır.

- 15 UCLA (no date) What is data mining? <http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm> [Erişim 20 Ekim 2016].
- 16 ABD Vatanseverlik Yasası ile ilgili detaylar için bkz. Electronic Privacy Information Centre (no date) USA Patriot Act. <http://epic.org/privacy/terrorism/hr3162.html> [Erişim 20 Ekim 2016].
- 17 Sosyal paylaşım siteleri ile ilgili gizlilik odağı ve kaygı, medyanın medeni haklarının savunucularının Facebook'ta gösterdiği özenli izleme ve baskıyla çok iyi bir şekilde gösteriliyor. Bu platformun kullanımıyla ilgili olarak ortaya çıkan çok çeşitli gizlilik konularına genel bir bakış için, bkz. Wikipedia (2012) Facebook Eleştirisi. http://en.wikipedia.org/wiki/Criticism_of_Facebook [Erişim 20 Ekim 2016].
- 18 Örnek olarak, Ağustos 2016'da, Facebook'un sahip olduğu mesajlaşma servisi WhatsApp, gizlilik politikasını değiştirdi; böylece kullanıcı, WhatsApp'ın Şartlar ve Koşullarını kabul ettiğinde, reklam hedefleme de dahil olmak üzere, verilerini doğrudan Facebook ile paylaşmayı otomatik olarak kabul ediyor. Veri paylaşımından çıkmak, değişiklik yapıldığı sırada tamamen mümkün görünmüyordu, ancak WhatsApp, verilerin hedefleme amacıyla Facebook tarafından kullanılmasına ilişkin kısmi bir seçim yapmayı teklif etti. Detaylar için bkz. Lamas N (2016) WhatsApp to share user data with Facebook for targeting – here's how to opt out. Techcrunch, 25 Ağustos. <https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-here-how-to-opt-out/> [Erişim 20 Ekim 2016].
- 19 Zaman içinde öne çıkan gizlilik ihlallerine genel bir bakış için bkz. Lord N (2016) The History of Data Breaches. Digital Guardian, 12 Ekim. <https://digitalguardian.com/blog/history-data-breaches> [Erişim 20 Ekim 2016].
- 20 The Economist (2004) Move over, Big Brother. 2 December. <http://www.economist.com/node/3422918> [Erişim 30 Ekim 2016].
- 21 Gov.track.us (no date) Video Voyeurism Prevention Act. <https://www.govtrack.us/congress/bills/108/s1301/text> [Erişim 20 Ekim 2016].
- 22 Council of Europe (1981) Convention for the protection of individual with regard to automatic processing of personal data. <http://conventions.coe.int/treaty/en/treaties/html/108.htm> [Erişim 20 Ekim 2016].
- 23 European Union (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 Ekim 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046> [Erişim 20 Ekim 2016].
- 24 European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679> [Erişim 27 Ağustos 2016].
- 25 OECD (2013) Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. <http://www.oecd.org/sti/economy/privacy.htm> [Erişim 30 Ekim 2016].
- 26 CJEU (2015) Judgement of the Court in Case C-362/14: Maximilliam Schrems v Data Protection Commissioner. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015> [Erişim 21 Ekim 2016].
- 27 European Commission (2016) Commission Implementing Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield. <http://eur-lex.europa.eu/legal-content/EN/TXT/?u->

- ri=OJ%3AJOL_2016_207_R_0001 [Erişim 21 Ekim 2016].
- 28 United Nations (1989) Convention on the Rights of the Child. <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx> [Erişim 21 Ekim 2016].
- 29 UN Human Rights Council (2012) Resolution A/HRC/20/L.13. The promotion, protection and enjoyment of human rights on the Internet. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [Erişim 21 Ekim 2016].
- 30 Livingstone S and Bulgar M (2014) A global research agenda for children's rights in the digital age. *Journal of Children and Media* 8(4). <http://www.lse.ac.uk/media@lse/WhosWho/AcademicStaff/SoniaLivingstone/pdf/Livingstone-&-Bulgar-JOCAM-A-global-research-agenda-for-childrens-rights-in-the-digital-age.pdf> [Erişim 18 Ağustos 2016].
- 31 CRC makalelerinin dijital ortama nasıl uygulandığının bir analizi için bkz: Livingstone S and Bulgar M (2014), *ibid*, and Livingstone S and O'Neill B (2014). Children's rights online: Challenges, dilemmas and emerging directions. In S. van der Hof et al. (Eds) *Minding Minors Wandering the Web: Regulating Online Child Safety*. Berlin: Springer.
- 32 Değerli yorumlar ve girdiler, Buenos Aires Ulusal Teknoloji Üniversitesi profesörü Jorge Plano tarafından sağlandı.
- 33 World Health Organization (2015) Disability and Health. Fact sheet No. 352. <http://www.who.int/mediacentre/factsheets/fs352/en/> [Erişim 21 Ekim 2016].
- 34 Disabled World (no date) Disability Statistics: Facts & Statistics on Disabilities & Disability Issues. <https://www.disabled-world.com/disability/statistics/> [Erişim 21 Ekim 2016].
- 35 United Nations (2006) Convention on the Rights of Persons with Disabilities. <http://www.un.org/disabilities/convention/conventionfull.shtml> [Erişim 21 Ekim 2016].
- 36 Erişilebilirlik ve Engellilik Konusunda IGF Dinamik Koalisyon, bir dizi erişilebilirlik kılavuzu geliştirmiştir. Bkz. <http://www.intgovforum.org/cms/dynamiccoalitions/80-accessibility-and-disability#documents> [Erişim 10 Ağustos 2016].
- 37 ITU (2016) ICT Facts and Figures 2016. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> [Erişim 21 Ekim 2016].
- 38 Web Foundation (2015) Women's Rights Online: Translating Access into Empowerment. Available at <http://webfoundation.org/about/research/womens-rights-online-2015/> [Erişim 12 Ağustos 2016].
- 39 United Nations (2016) Report of the Special Rapporteur on violence against women, its causes and consequences. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/42 [Erişim 7 Kasım 2016]

Bölüm 9

İnternet yönetiřimi aktörleri

İTERNET YÖNETİŞİMİ AKTÖRLERİ

İnternet yönetiřimi, (WSIS 2003 **İlkeler Bildirimi**'nin 49. paragrafında ve WSIS 2005 **Tunus Bilgi Toplumu Gündemi**'nin 35 ve 36. paragraflarında belirtildiđi gibi) ulusal hükümetler, uluslararası kuruluşlar, iş dünyası, sivil toplum ve akademik ve teknik topluluklar dahil olmak üzere sıkça adlandırıldıđı gibi çok çeřitli aktörleri veya paydařları içermektedir. Çok paydařlık, WSIS belgelerinde bir yönetiřim ilkesi olarak kabul edilirken, asıl tartiřma, esas olarak İnternet yönetiřiminin çeřitli alanlarındaki devlet ve devlet dıřı aktörler arasındaki iliřkiye odaklanarak, her bir aktörün kendine özgü rolleri ve sorumlulukları üzerine olmaktadır.

İnternet yönetiřim aktörlerinin çođu, diđerlerinin yanı sıra teknolojik, yasal, ekonomik, insan hakları ve sosyokültürel yönleri içeren, konularının multidisipliner doğası ile karakterize olan bu alanın yüksek karmařıklıđı ile başa çıkmakta zorlanmaktadır. Ayrıca, İnternet yönetiřimi sorunları yerel, ulusal, bölgesel ve küresel olmak üzere farklı politika seviyelerinde ele alınmaktadır. Bu bölüm, İnternet yönetiřim aktörlerinin bir incelemesi ve onların herbirinin konumlarının bir özetini sunmaktadır.

İnternet yönetiřimi ve diđer küresel politika süreçleri arasındaki kavramsal fark nedir?

İnternet yönetiminde, hükümetler IETF, İnternet Topluluđu ve ICANN etrafında kurulmuş halihazırda var olan bir hükümet dıřı rejime dahil olmak zorunda kalmıřlardır. İklim deđiřikliđi, ticaret, göç gibi diđer politika alanlarında bunun tersi olmuřtur. Hükümetlerarası politika alanı kademeli olarak sivil toplum aktörlerine açılmaktadır. WSIS 2003'ten bu yana, birçok hükümet İnternet yönetiřimi sahnesine girmeye bařladıđında, asıl zorluk hükümet dıřı İnternet yönetiřimi rejimini ve geleneksel diplomatik alanı senkronize etmek olmuřtur. Bu yakınsama, hükümetlerin ve İnternet yönetiřimindeki diđer aktörlerin rolleriyle ilgili ana tartiřmaları tetiklemiş, aynı zamanda daha kapsayıcı ve etkili politika oluřturma konusunda fırsatlar yaratmıřtır.

Hükümetler

Modern çağın tanımlayıcı teknolojisi olan İnternet, devletlerin (ulusal güvenlik meselesine odaklanan) jeopolitiklerini ve gittikçe artan bir řekilde (ekonomik çıkarlarla ulusal çıkarların teřvik edilmesi olarak tanımlanan) jeoekonomilerini etkilemektedir. İnternet ayrıca, müzakere ve iřbirliđi yoluyla politika çözümlerini belirleme ihtiyacını tetikleyen yüksek düzeyde ekonomik ve sosyal dayanıřma yaratmaktadır. WSIS sürecinde, küresel diplomatik gündemde 2003–2005 yıllarında İnternet yönetiřimi ortaya çıkmıřtır. O zamandan beri, birçok hükümet bu karmařık politika alanını kavramaya çalıřmaktadır.

İnternetin dünya çapındaki ulusal toplumlar için kritik önemi, ulusal düzeyde etkili İnternet yönetiřimi geliřtirmek ve dijital alanda çıkarlarını korumak için İnternet diplomasisi çabalarına katılmaları için hükümetler üzerinde ek bir baskı oluřturmuřtur.

Hükümetlerin uluslararası çabaları iki ana yöne kanalize etmiřlerdir. İlk olarak, hükümetler İnternet'i, yeni bir politika konusu olarak, ICANN ve IGF gibi çok paydařlı olanlardan ITU

ve BM GGE gibi çok taraflı olanlara kadar geniş bir alanda ele almaktadır (örneğin, Tablo 3 hükümetlerin BM GGE'ye katılımını göstermektedir). İkincisi, hükümetler ticaret (DTÖ bağlamında), sağlık (WHO) ve emek (ILO) gibi geleneksel politika konularının dijital yönleriyle ilgilenmek zorundadır.

Büyük ve zengin ülkeler için bile, İnternet yönetişimi konularıyla uğraşmak, İnternet yönetişiminin (teknolojik, ekonomik ve sosyal yönler gibi) çok disiplinli doğasının yönetimi ve çok çeşitli aktörlerin katılımı gibi çeşitli zorluklarla karşılaşmışlardır. Birçok hükümetin aynı anda yetkilileri eğitmesi, politika geliştirmesi ve uluslararası İnternet ile ilgili farklı toplantılara aktif olarak katılması gerekmiştir.

Ulusal koordinasyon

2003 yılında, WSIS sürecinin başlangıcında, çoğu ülke, telekomünikasyon meseleleriyle ilgilenen başlıca uluslararası kuruluş olan ITU ile ilişkilerden sorumlu olan telekomünikasyon bakanlıkları ve düzenleyici otoriteler aracılığıyla İnternet yönetişimi konularına eğilmiştir. İnternetin modern toplumun politik, sosyal ve ekonomik yapısı üzerindeki etkisinin artması ile birlikte yavaş yavaş, dış ilişkiler, kültür, medya ve adalet de dahil olmak üzere diğer devlet daireleri de İnternet yönetiminde yer almaya başlamıştır.

Birçok hükümet için asıl zorluk, genellikle İnternet yönetim sorunları ile ilgilenmek için gerekli uzmanlığa sahip olan üniversiteler, özel şirketler ve STK'lar gibi devlet dışı aktörlerden destek toplamak ve bunları etkin bir şekilde koordine etmek için bir strateji geliştirmek olmuştur. WSIS 2003'ten sonraki yıllarda, çoğu büyük ve orta ölçekli G20 ülkesi, küresel İnternet yönetişimi müzakerelerini takip etmek için yeterli kurumsal kapasite geliştirmeyi başarmıştır. Brezilya gibi bazıları, telekomünikasyon bakanlıkları, diplomatik hizmet, iş sektörü, sivil toplum ve akademi gibi İnternet yönetişimi tartışmalarını takip etmek için yenilikçi ulusal yapılar geliştirmiştir.¹ Hindistan, Endonezya ve Kenya, ulusal düzeyde çok paydaşlı işbirliği geliştiren ülkelerin diğer örnekleridir. Birçok ülke, ulusal IGF girişimlerini, çeşitli paydaş gruplarını İnternet yönetimi ve dijital politika süreçlerine dahil etmenin bir yolu olarak kullanmaktadır. Ekim 2016'da, küresel IGF Sekreteryası tarafından tanınan 47 ulusal IGF girişimi olmuştur.²

Politika uyumu

İnternet yönetişiminin çok disiplinli doğası ve aktörlerin ve politika forumlarının çeşitliliği göz önüne alındığında, politika tutarlılığını sağlamak özellikle zordur. Örneğin, mahremiyet ve veri koruma sorunu, diğerlerinin yanı sıra, insan hakları, ticaret, standardizasyon ve güvenlik perspektiflerinden ele alınmakta, ancak çoğu zaman, her perspektifle ilgilenen politika ve uzman grupları arasında çok az koordinasyon bulunmaktadır (Şekil 26). İnternet yönetişimi alanında politika tutarlılığının sağlanması, farklı bakanlıklar, iş sektörü ve diğer aktörler arasındaki yatay iletişimi içeren esnek bir politika koordinasyonu biçimini gerektirir.

Kablo jeo-stratejisi ve politikası tutar(sız)lılığı

Anglo Fransız Anlaşması³ 1904'te oluşturuldu. Bununla birlikte, Almanya ile yakın işbirliğinin kurulmasında, Fransız Telgraf Bakanlığı, ülkenin İngiltere ile ilişkilere yönelik dış politikası tercihini takip etmemiştir. Bunun ana nedeni, Almanya ile işbirliği içinde yeni telgraf kabloları döşerken küresel kablo coğrafyası stratejisinde İngiliz hakimiyetini azaltmak olmuştur. 1915'te Fransız tarihçi Charles Lesage, bu politika tutar(sız)lılığı üzerine şu yorumu yapmıştır: 'Fransız diplomasisinin genel ilkeleri ile telgraf politikalarının prosedürleri arasındaki uzun süredir devam eden anlaşmazlıkların, bu ülkede her bakanlığın kendi dış politikası olmasından kaynaklandığına inanıyorum: Dışişleri Bakanlığı'nın bir, Maliye Bakanlığı'nın bir başkası dış politikası vardır ... Posta ve Telgraf İdaresi'nin de zaman zaman kendi dış politikası vardır; bu böyle iken, son birkaç yılda, Fransız diplomasisi İngiltere'ye tamamen düşmanca davranmadan, Almanya'ya güçlü bir yaklaşım göstermiştir.'⁴

Yönetim zorluklarının dışında, politika tutarlılığının elde edilmesi, genellikle rekabet eden politika çıkarlarının varlığı ile sınırlıdır. Bu, özellikle gelişmiş ve çeşitlendirilmiş İnternet ekonomilerine sahip ülkelerde geçerlidir. Örneğin, ağ tarafsızlığı tartışmasının başında, çeşitli ülkelerdeki düzenleyiciler, ağ tarafsızlığını destekleyen İnternet endüstrisi ile ağ tarafsızlığını örneğin multimedya içeriğinin yayınlanması için daha hızlı İnternet üzerine bir iş modeli geliştirmeye engel olarak gören telekomünikasyon ve eğlence sektörleri arasında bir denge kurmaya çalışmışlardır.



Şekil 26. Dijital alanda köprü oluşturma politika siloları

İnternet yönetiminde Cenevre merkezli daimi misyonların rolü

Birçok hükümet için Cenevre'deki daimi misyonları, hayati olmasa da, WSIS ve İnternet yönetim süreçlerindeki oyuncular için önemlidir. İnternet yönetişimi ile ilgili faaliyetlerin birçoğu, WSIS süreçlerinde öncü rol alan ITU'ya ev sahipliği yapan Cenevre'de gerçekleştirilmiştir. Hazırlık toplantılarından birisi dışındaki tüm toplantılara kalıcı misyonların dahil olduğu WSIS'nin ilk aşaması, 2003'te Cenevre'de gerçekleşmiştir. Halen, IGF Sekreteryası Cenevre'de bulunmakta ve orada birçok IGF hazırlık toplantısı düzenlemektedir.

Büyük ve gelişmiş ülkeler için, Cenevre merkezli kalıcı misyonlar, WSIS ve İnternet yönetim süreçleriyle ilgilenen kurum ve bireylerden oluşan geniş bir ağının parçası olmuştur. Kalıcı misyonlar küçük ve gelişmekte olan ülkeler için birincil ve bazı durumlarda bu ülkelerin süreçlerdeki tek oyuncuları olmuştur. İnternet yönetişimi sorunları genellikle gelişmekte olan ülke denemelerinin küçük ve genişletilmiş misyonlarının gündemine eklenmiştir. Birçok durumda, aynı diplomat, insan hakları, sağlık, ticaret ve emek gibi diğer konuların yanı sıra İnternet yönetim süreçleriyle ilgili görevleri de üstlenmek durumundadır.

Ulusal hükümetlerin konumu

Amerika Birleşik Devletleri

İnternet, ABD hükümetinin desteklediği bir bilimsel projenin parçası olarak geliştirilmiştir. İnternetin başlangıcından günümüze kadar, ABD hükümeti başlangıçta Savunma Bakanlığı, daha sonra Ulusal Bilim Vakfı ve en son Ticaret Bakanlığı olmak üzere farklı departmanlar ve kurumlar aracılığıyla İnternet yönetişimine dahil olmuştur. FCC ayrıca İnternet düzenleyici çerçevenin oluşturulmasında önemli bir rol oynamıştır.

ABD hükümetinin katılımının kalıcı bir unsuru, genellikle “uzak bir vesayet” olarak nitelendirilen ‘kapalı yaklaşım’dır. İnternetin yönetişimini, doğrudan onunla çalışanlar bir yana, temelde teknik topluluğa bırakmıştır. Bununla birlikte, ABD hükümeti, kar amacı gütmeyen Kayıt Kurulları Konseyi (CORE) projenin kök sunucusunu ve çekirdek İnternet altyapısının yönetimini ABD’den Cenevre’ye taşıması gündeme geldiğinde 1990’ların ortalarında olduğu gibi birkaç defa daha doğrudan müdahale etmiştir.⁵ Bu süreç ABD Dışişleri Bakanı Madeleine Albright tarafından ITU Genel Sekreteri’ne gönderilen ünlü (en azından İnternet tarihinde) diplomatik bir notla durdurulmuştur.⁶ CORE girişimini durdurmaya paralel olarak, ABD hükümeti, 1998 yılında ICANN’ın kurulmasıyla sonuçlanan istişareler başlattı. ICANN, ABD hükümeti tarafından (özellikle DNS ve IP numaraları gibi) tanımlayıcılar gibi IANA işlevlerini yerine getirme, yani İnternet’in benzersiz sistemlerini koordine etme görevini üstlenmiştir. ABD hükümeti, bu rolün küresel İnternet topluluğuna geçtiği IANA işlevlerinde Ekim 2016’ya kadar bir liderlik rolü üstlenmiştir.

İyi gelişmiş çevrimiçi alanı ve canlı İnternet endüstrisi, ABD’yi siber güvenlik saldırılarına karşı özellikle savunmasız hale getirmektedir. Dolayısıyla ABD diplomasisi uluslararası siber güvenlik müzakerelerinde çok aktiftir. ABD, kendini savunma hakkı gibi mevcut güvenlik normlarının da İnternete uygulanması gerektiği fikrini desteklemektedir. Ülke, küresel bir siber güvenlik

anlaşmasının kabulüne karşı çıkmaktadır. ABD, çok çeşitli bölgesel ve ikili siber güvenlik anlaşmalarına taraftır. ABD, Siber Suçlar Konvansiyonu Sözleşmesi ve MLAT'lar dahil olmak üzere ikili anlaşmalar yoluyla uluslararası siber suçlarla ilgilenmektedir. ABD ayrıca, örneğin mevcut CERT'lerin kurulması veya güçlendirilmesi yoluyla siber güvenlik yapılarının geliştirilmesini de desteklemektedir.

Ekonomik konularda ABD, serbest veri akışını ve dijital hizmetlerle serbest ticareti desteklemektedir. DTÖ'de ve çeşitli bölgesel ve ikili ticaret anlaşmalarıyla ücretsiz çevrimiçi ticaret teşvik edilmektedir. ABD İnternet endüstrisi, kritik bir unsur olan serbest veri akışı ile serbest veri ticaretinin en önemli yararlanıcısıdır. ABD çevrimiçi işlemlerin vergilendirilmesine karşı çıkmaktadır.

Avrupa Birliği

Avrupa Birliği, gelecekteki İnternet yönetiminde uzlaşma sağlamak için benzersiz bir sert ve yumuşak dijital güç karışımına sahiptir. AB'nin sert dijital gücü, hem yüksek İnternet penetrasyonuna (2015'de % 79,3)⁷ hem de satın alma gücüne sahip 500 milyon kişilik bir piyasanın çekiciliğine dayanmaktadır. Brüksel'deki İnternet endüstrisi lobisinin yoğunluğunun gösterdiği gibi, bu tür bir güç kaynağı önemlidir. Tekelleşme ve veri koruma konularında AB ile müzakere ederek, diğer şirketler arasında Google ve Facebook, (AB'nin İnternet endüstrisi ile yaptığı düzenlemeler çoğu zaman diğer ülkeleri ve bölgeleri ve benzer eylemlerde bulunmaya teşvik ettiği için) bir anlamda dünyanın geri kalanıyla da müzakere etmektedir. Örneğin Google'ın, Avrupa Ekonomik Alan'ındaki çevrimiçi arama pazarının % 90'ından fazlasına sahip olduğu bir durumda, AB, Google'ın Avrupa'da yüksek pazar payının şirketin baskın pazar pozisyonunun kötüye kullanılması da dahil muhtelif uygulamalarla kötüye kullanılmasını engelleyecek temel oluşum olarak konumlandırılmaktadır.⁸

AB'nin yumuşak dijital gücü, zayıf yönleri güçlü hale getirmek için bir tür dijital aikido diplomasisine dayanıyor. AB güçlü bir İnternet endüstrisine sahip olmasa da, bu zayıflık paradoksal olarak İnternet yönetiminde bir güç haline getirilebilir.

Yani, İnternet endüstrisinin ekonomik çıkarlarını korumaya gerek kalmadan, AB (kullanıcı hakları, dahil etme, içerik çeşitliliği gibi) kamu çıkarlarını ortaya koymak ve korumak bakımından daha fazla özgürlüğe sahiptir. Bu şekilde, AB "İnternet kullanıcıları"nın koruyucusu ve İnternet endüstrisinin büyümesi için uygun bir ortamın destekçisi olabilir. AB, uluslararası politikada çoğu zaman geçerli olmayan hem etik hem de stratejik hedeflere ulaşabilir.

Farklı meseleye dayalı ittifaklar geliştirme konusunda AB yaklaşımı ortaya çıkmaya başlamıştır. WCIT-12'de, Avrupa ABD'yi desteklemiştir. Veri koruma ve mahremiyet konusunda AB'nin konumu Latin Amerika ülkelerinin pozisyonuna yakındır. İsviçre ve Norveç çoğu İnternet yönetimi konusunda AB ile benzer bir konumdadır.

Önümüzdeki dönemde, AB'nin İnternet yönetimindeki konumu, özellikle vergilendirme, müşterinin korunması ve veri akışı gibi alanlarda olmak üzere, AB Dijital Tek Pazarının gelişimi ile daha da şekillenecektir.

AB üye ülkeleri belirli İnternet yönetiřimi konularına önem vererek bunların konum alanlarını geliřtirmektedir. Almanya ve Avusturya özellikle mahremiyet ve veri koruma konusunda endiře duymakta, bu nedenle hem AB hem de BM sistemi iinde evrimii mahremiyet koruması konusundaki tartiřmalarda lider rol oynamaktadırlar.

Estonya ok dinamik bir dijital politika oyuncusudur. İnterneti ciddi dzeyde etkileyen 2007 DDoS saldırısından sonra Estonya, siber uzmanlık alanında ok aktif bir oyuncu haline gelmiřtir. NATO'nun **Kooperatif Siber Savunma Mkemmeliyet Merkezi**'nin yanı sıra, 2010'dan beri her yıl dzenlenen byk bir siber gvenlik etkinlięi olan **Siber atıřma Konferansına** ev sahiplięi yapmaktadır.

Romanya siber sularla mcadele alanında uzmanlařmıřtır. Amacı lkelerin su adalet sistemlerini glendirmelerine ve siber suun getirdięi zorluklara cevap verme kapasitelerini Siber Sular Konvansiyonu standartlarına dayanarak destekleme olan **CoE Siber Sular Programı Ofisine** ev sahiplięi yapmaktadır.

Hollanda, **Siber Uzmanlık Kresel Forumu**'na ve siber gvenlik alanındaki dięer birok giriřime ev sahiplięi yapmaktadır.

in

in, dnyadaki en yksek sayıda İnternet kullanıcısı olan (700 milyondan fazla) ve (on byk İnternet řirketinden drd in'den olmak zere) hızlı byyen bir İnternet endstrisi lkesi olarak İnternet ynetiminde nemli bir oyuncudur. in, ulusal politikaların tesinde sınırsız İnternet iletiřimine karřı ekonomik gdml yaklařım ile ulusal dzeyde İnternet faaliyetleri iin politik gdml siber egemenlik yaklařımı arasındaki dijital politikadaki konumunu dengelemektedir.

Ekonomik aıdan bakıldıęında, kresel İnternet in'in ihracata ynelik ekonomisi iin hayati neme sahiptir. inli řirketler interneti dnya apındaki ticari faaliyetlerinde bilgi altyapısı olarak kullanmaktadır. in'deki iřletmeler iin ana İnternet platformu olan Alibaba, řu anda dnya genelinde en yksek e-ticaret iřlem hacmine sahiptir. Alibaba'nın sahibi Jack Ma, KOBİ'lerin kresel dijital ticaret yapmalarına yardımcı olmak amacıyla bir Elektronik Dnya Ticaret Platformu kurulması aęırısında bulunmuřtur.⁹ Hangzhou'daki G20 toplantısında, Eyll 2016'da in, dijital ekonomiyi ve inovasyonu gl řekilde desteklemiřtir.

Siyasi bir perspektiften, egemenlięin in dıř politikasının temel tařı olarak korunması da siber ortamda yansıtılmaktadır. in cumhurbaşkanı Xi, 2015 Dnya İnternet Konferansında siber egemenlięi, "her bir lkenin baęımsız bir řekilde kendi siber geliřim yolunu, siber dzenleme modelini ve İnternet kamu politikalarını seme ve uluslararası siber ynetiřimine eřit katkıda bulunma" hakkı olarak nitelendirmiřtir.¹⁰ Siber egemenlik yaklařımına gre, İnternet, ulusal sınırları olan fiziksel alanın yasalarını, geleneklerini ve ynetiřimini takip etmelidir.

in, yabancı İnternet řirketlerin in pazarına eriřimi kısıtlayarak (Facebook, Google, Twitter) ve bunun yerine in řirketleri tarafından benzer hizmetlerin sunulmasını teřvik ederek yksek dzeyde bir siber egemenlik elde etmiřtir: Baidu (Google'ın eřdeęeri), Sina Weibo (Twitter'ın

eşdeğeri), Renren (Facebook'un eşdeğeri), Youku (YouTube'un eşdeğeri). Çinli bireylere ve kurumlara ait verilerin çoğu, Çin'deki sunucularda depolanmaktadır. Çin'in siber egemenliğinin eleştirel görüşleri, hükümetin halka yayılmasının uygun olmadığını düşündüğü çevrimiçi içeriğin filtrelmesi ile ilgilidir.

Küresel dijital politika alanında, Çin genellikle çok taraflı bir yaklaşımı desteklemektedir. Bununla birlikte, ICANN ve IETF gibi çok paydaşlı süreçlere ve organlara da aktif olarak katılmaktadır. Uluslararası dijital politikaya daha aktif olarak katılma çabalarının bir parçası olarak Çin, 2014'ten beri yıllık bir Dünya İnternet Konferansı'na ev sahipliği yapmaktadır.

Önümüzdeki dönemde, Çin'in dış dijital politikası, Asya ve Avrupa arasındaki dijital bağlantıyı arttırmayı amaçlayan Dijital İpek Yolu'nun gelişimini destekleyecektir. Dijital İpek Yolu, Çin ve Avrupa'yı çok sayıda kara ve deniz bağlantısıyla birbirine bağlayan [Bir Kemer, Bir Yol](#) olarak bilinen daha geniş bir projenin parçası olacaktır.

Brezilya

[Brezilya](#), küresel dijital politikadaki en aktif ülkelerden birisidir ve Latin Amerika'daki en büyük internet pazarıdır. Canlı dijital alana sahip demokratik ve gelişmekte olan bir ülke olarak Brezilya, İnternet yönetişimi tartışmalarında (hükümetler arası ve hükümet dışı olmak üzere) iki kamp arasında bir uzlaşma sağlama potansiyeline sahiptir. Brezilya'nın bu rolü güçlü bir diplomatik girişimde bulunduğu Snowden'in ifşaatlarının ardından ortaya çıkmıştır. 68'inci UNGA Oturumu'ndaki konuşmasında Brezilya Devlet Başkanı Dilma Rousseff şunu ifade etmiştir: 'Birleşmiş Milletler Devletlerin bu teknolojilerle ilgili davranışlarını düzenleme çabasında lider bir rol oynamalıdır.' Ayrıca, gözetimi 'uluslararası hukuka aykırılık' ve 'Brezilya'nın ulusal egemenliğine saygısızlık' olarak tanımlamıştır.¹¹ Brezilya'nın hükümetler arası bir yaklaşım konusunda ısrarcı olduğu görüldüğünde, Başkan Rousseff, çok paydaşlı İnternet yönetişimi modelini daha da geliştirmeyi amaçlayan NETmundial toplantısını organize etmeyi önererek politika spektrumunun merkezine geri dönmüştür. Brezilya, asıl amacının, toplantıdan (bağlayıcı olmayan) başarılı bir sonuç elde etmeyi sağlamak için karmaşık bir role sahip olmuştur.¹²

Brezilya çok sayıda dijital politika sürecinde oldukça aktiftir. Ülke, 10 IGF toplantısından ikisine ev sahipliği yapmıştır. WSIS + 10 görüşmelerinde lider bir rol oynamıştır. Brezilya, Almanya ile birlikte, çevrimiçi mahremiyetin uluslararası çerçevede korunmasının güçlü bir destekleyicisi olmuştur.

Hindistan

[Hindistan](#) dijital politikada önemli bir oyuncudur. Ülke geniş bir İnternet kullanıcı tabanına ve gelişmiş bir İnternet endüstrisine sahip olmakla birlikte, sayısız nüfusuna erişim sağlama konusunda da zorluklarla karşılaşmaktadır. Hindistan'ın karmaşık İnternet yönetim politikası, ulusal dijital politika oluşturma konusundaki karmaşıklığı da yansıtmaktadır. Küresel İnternet yönetiminde en çeşitli ve canlı sivil toplum sahnelerinden birine sahiptir. Geçmişte, Hindistan hükümeti İnternet yönetişimi için hükümetler arası bir yaklaşıma yönelmişken, iş dünyası ise

hükümet dışı bir yaklaşıma daha yakın olmuştur. Bu ikilem bazı şaşırtıcı hamlelere yol açmıştır. Örneğin, Hindistan, CIR'in hükümetler arası denetimini sağlamanın bir yolu olarak BM İnternet ile İlgili Politikalar Komitesi'nin kurulmasını önermiştir. Hindistan, gelişmekte olan ülkelerin çoğunda olduğu gibi, değiştirilmiş ITR'leri imzalamadığı için gelişmiş ülkelerle birlikte yer aldığı WCIT-12'deki İnternet politikaları yelpazesinin diğer tarafına geçmiştir. Mevcut Hint yönetimi, Kasım 2016'da Hindistan'da düzenlenen ICANN 57 toplantısında yinelenen çok paydaşlı İnternet yönetişimi modelini desteklemektedir.¹³

Rusya

Rusya, İnternet ile ilgili kamu politikası konularını ele almada hükümetlerin lider rolü oynayarak İnternet yönetişimine çok taraflı bir yaklaşımın en sesli ve tutarlı destekçisi olmuştur. Özellikle Rusya, ITU'nun İnternet yönetimi alanındaki rolünü desteklemektedir. Siber güvenlik alanında, Rusya, 1998'de BİT ve güvenlik ile ilgili ilk UNGA kararının ne olacağı konusunda bir teklif hazırladığında ilk adımları atmıştır.¹⁴ 1998'den bu yana, bu karar her yıl tekrarlanmaktadır ve UNGA'nın ilk komitesinin ve son olarak da BM GGE'nin çalışmaları yoluyla siber güvenliğin ele alınmasına yol açmıştır.¹⁵ Rusya, Çin, Kazakistan, Kırgızistan, Tacikistan ve Özbekistan ile birlikte, diğer kurumsal alanlarda da siber işbirliğini sürdürmektedir. Özellikle, SCO çerçevesinde, uluslararası bilgi güvenliği ile ilgili bir 2009 anlaşması bulunmaktadır.

Rusya, Eylül 2015'te, Rus internet kullanıcılarının verilerini Rusya sınırları içinde saklanmasını gerektiren bir veri yerleştirme düzenlemesi getirmiştir. Bu yasa, (Facebook, Twitter, Google, LinkedIn gibi) büyük İnternet şirketlerini sunucularını ya Rusya'ya yerleştirmeye ya da hizmetlerinin Rusya topraklarında engellenme riskini almaya zorlayabilir.

Ülkeler	Yıl	2004-2005	2009-2010	2012-2013	2014-2015	2016-2017
Arjantin						
Avusturya						
Belarus						
Botswana						
Brezilya						
Kanada						
Çin						
Kolombiya						
Küba						
Mısır						
Estonya						
Finlandiya						
Fransa						
Almanya						
Gana						
Hindistan						
Endonezya						
İsrail						
İtalya						
Japonya						
Ürdün						
Kazakistan						
Kenya						
Malesya						
Mali						
Meksika						
Hollanda						
Pakistan						
Katar						
Kore Cumhuriyeti						
Rusya Federasyonu						
Senegal						
Sırbistan						
Güney Afrika						
İspanya						
İsviçre						
ABD						
İngiltere						

Tablo 3. 2004'ten beri kurulmuş olan beş BM GGE'sine üyelik araştırması

Kenya

Kenya, internet yönetiminde en dinamik oyuncular arasında yer almaktadır. Ulusal bir IGF ile sivil toplumun, iş dünyasının ve akademinin aktif şekilde İnternet yönetişimi üzerindeki hükümet destekli girişimlere katılımıyla enerjik bir çok paydaşlı görünüme sahiptir.

Kenya'nın temel başarılarından biri, milyonlarca kişiye finansal hizmetlere erişim sağlayan MPesa ödeme sistemi olmuştur. Sistem, diğer ülkelere ihraç edilirken, ulusal İnternet sektörüne de büyük bir destek sağlamıştır.

Kenya, Afrika ve küresel dijital politika süreçlerinde çok aktiftir. 2011'de düzenlenen yıllık IGF toplantısına ev sahipliği yapmıştır. Ayrıca Kenya hükümeti, iş dünyası ve sivil toplum temsilcileri, diğerleri arasında ITU, ICANN, IGF ve BM GGE'de çok aktif katılımcılar arasındadır.

Endonezya

Endonezya, İnternet'te çok hızlı bir büyüme kaydetmiş ve 2016 yılında 53 milyon kullanıcıya ulaşmıştır. Endonezya için, bir takımada ülkesi olarak, İnternet, 6000'den fazla yerleşik adaya bağlanan kritik bir altyapıdır.

Endonezya'da devlet kurumları, ticari kuruluşlar, akademi ve sivil toplum temsilcilerini bir araya getiren ulusal bir IGF bulunmaktadır. Güvenlik alanında, ülkenin temel kaygısı, İnternet'in terörist gruplar tarafından kullanılmasıyla ilgilidir. Ekonomik tarafta, Endonezya Google ve diğer internet şirketleri için özel bir vergi almayı düşünmektedir. Mahremiyet ve veri koruma alanında, Endonezya unutulma hakkını benimsemiştir. Avrupa'nın unutulma hakkı konusundaki (diğer bir deyişle, belirli içeriğin arama motoru sonuçlarından çıkarılmasına izin verilmesi anlamına gelen) anlayışına ek olarak, Endonezya ayrıca ilgisiz içeriği web sitelerinden silme olasılığını da dikkate almaktadır.

Endonezya, uluslararası dijital politikada aktif bir katılımcı olmuştur. 2013 yılında IGF'nin yıllık toplantısına ev sahipliği yapmıştır. Ülke ayrıca İTÜ, ICANN, IGF ve BM GGE faaliyetlerine aktif olarak katılmaktadır.

İsviçre

İsviçre, Cenevre'deki ilk büyük olay olan 2003 WSIS aşamasından bu yana, küresel İnternet yönetim ekosisteminin gelişiminde öncü bir rol oynamıştır. İsviçreli diplomat Markus Kummer, WGIG ve ardından IGF Sekreteryası'na (2010 yılına kadar) liderlik etmiştir. ICANN'ın GAC'ine 2014'ten beri İsviçre Federal İletişim Ofisi'nde görevli Thomas Schneider başkanlık etmektedir.

Siber güvenlik alanında İsviçre, siber alan için CBM'lerin gelişimine aktif bir katkıda bulunmuştur. Halen, İsviçre BM GGE'nin bir üyesidir (2016-2017).

İnsan hakları alanında İsviçre, çevrimiçi alanda mahremiyetin korunmasını BM ve diğer uluslararası mekanizmalar aracılığıyla aktif olarak destekleyen ülkeler arasındadır.

Küçük devletler

Sorunların karmaşıklığı ve faaliyetlerin dinamikliği, birçok küçük ülkenin, özellikle küçük gelişmekte olan ülkelerin, İnternet yönetişimi politika süreçlerini takip etmesini neredeyse imkansız hale getirmiştir. Sonuç olarak, bazı **küçük devletler** İnternet yönetimi sorunları için tek duraklı hizmet yapısını desteklediler.¹⁶ Gündemin büyüklüğü ve gelişmekte olan ülkelerin hem kendi ülkelerindeki hem de diplomatik misyonlarındaki sınırlı politika kapasitesi bu süreçte tam katılımlarının önündeki temel engellerden birisidir. İnternet yönetişimi ve politikası alanında kapasite geliştirme ihtiyacı, **WSIS Tunus Bilgi Toplumu Gündemi** için önceliklerden biri olarak kabul edilmiştir.

İnternet yönetişimi - değişken bir geometri yaklaşımı

İnternet yönetişimi, uluslararası yasal kapasite, özel İnternet yönetişimi konularına ilgi ve mevcut uzmanlık dahil olmak üzere pek çok açıdan farklılık gösteren çeşitli paydaşların katılımını gerektirir. Bu çeşitlilik, ana paydaşlar için aşağıdaki rolleri belirten WSIS İlkeler Bildirgesi'nin¹⁷ 49'uncu paragrafında belirtilen değişken geometri yaklaşımı kullanılarak ele alınabilir:

- Devletler - 'İnternet ile ilgili (uluslararası yönler dahil) kamusal meselelerde politika yapıcı otorite'.
- Özel sektör - 'İnternet'in hem teknik hem de ekonomik alanlarda geliştirilmesi'.
- Sivil toplum - 'İnternet konularında özellikle toplum düzeyinde önemli rol'.
- Hükümetlerarası kuruluşlar - 'İnternet ile ilgili kamu politikaları meselelerinin koordinasyonu'.
- Uluslararası kuruluşlar - 'İnternet ile ilgili teknik standartlar ve ilgili politikaların geliştirilmesi'.

Değişken geometri yaklaşımı pratikte ortaya çıkmaya başlamıştır. Örneğin, devletler siber güvenlik ve e-ticarette lider bir rol üstlenirken, teknik ve ticari topluluklar standardizasyon ve İnternet isimlerinin ve numaralarının yönetiminde lider rollere sahiptir.

İş dünyası¹⁸

İnternetin ilk günlerinde, iş sektörünün temel kaygısı, şirketlerin siber baskıyla karşı karşıya kalması ve ticari markalarının ilk önce alan adı olarak kaydedilmeleri için yeterince hızlı olan kişiler tarafından kötüye kullanılması nedeniyle ticari markaların korunması ile ilgilidir. ICANN 1998'de kurulduğunda, iş çevreleri açıkça ticari markaların korunmasına ilişkin önceliklere sahipti. İnternet ve e-ticaretin büyümesi, iş sektörünün mahremiyet ve veri koruması ve diğer çevrimiçi insan hakları, siber güvenlik, e-bankacılık, vergi, içerik politikası ve çok dillilik gibi diğer alanlara olan ilgisini tetiklemiştir. Bugün, iş dünyası için doğrudan alakalı olmayan herhangi bir İnternet yönetişimi sorunu bulmak zordur. Ancak, belirli bir konuya yapılan vurgu, endüstriden endüstriye değişmektedir.

Uluslararası Ticaret Odası

Sektörler arası ve coğrafi sınırlardaki işletmeleri temsil eden ana dernek olarak bilinen ICC, kendisini küresel İnternet yönetim süreçlerinde işletme sektörünün ana temsilcilerinden biri olarak konumlandırmıştır. ICC, ilk WGIG müzakerelerine ve WSIS'e aktif olarak dahil olmuştur ve mevcut IGF süreçlerine aktif bir katkıda bulunmaya devam etmektedir.

İnternetin sürekli büyümesiyle birlikte, iş dünyasının internet yönetimine ilgisi geniş ve çeşitli olmuştur. Alan adı şirketleri, ISS'ler, telekomünikasyon şirketleri ve İnternet içeriği şirketleri gibi ana şirket grupları İnternet yönetim süreçlerine aktif olarak dahil olmuştur.

Alan adları şirketleri

Alan adı şirketleri, TLD'leri (ör. .Com ve .net) yöneten tescil şirketlerini ve alan adlarının son kullanıcılar tarafından kaydedilmesini kolaylaştıran kayıt şirketlerini içerir. Başlıca oyuncular arasında VeriSign ve Afiliyas vardır. Tescil ve kayıt şirketleri, ICANN'ın yeni TLD'lerin tanıtılması ve uyumsuzlukların çözümü gibi alanlardaki politika kararlarından doğrudan etkilenir. Bu da, onları ICANN politika oluşturma sürecindeki en önemli aktörlerden yapar. birçok tescil ve kayıt sicil şirketi bireysel olarak veya birlikler aracılığıyla daha geniş İnternet yönetişimi politika süreçlerinde (WSIS, WGIG, IGF) yer almıştır.

İnternet servis sağlayıcıları

İnternet Servis Sağlayıcıların kilit çevrimiçi araçlar olarak rolü, onları İnternet yönetişimi için özellikle önemli kılar. Başlıca ilgi odakları, hükümet ve kolluk kuvvetleriyle muhattap olma hususunda ulusal düzeydedir. Küresel düzeyde, özellikle ABD ve Avrupa'dan gelen bazı ISS'ler, bireysel olarak veya ulusal, bölgesel veya (Amerika Bilgi Teknolojileri Birliği (ITAA), Avrupa İnternet Servis Sağlayıcıları Birliği (EuroISPA) ve diğerleri gibi) sektöre özgü kurumlar yoluyla, WSIS, WGIG, IGF ve ICANN süreçlerinde aktif olmuştur.

Telekomünikasyon şirketleri

Telekomünikasyon şirketleri, İnternet trafiğini kolaylaştırmakta ve İnternet altyapısını işletmektedir. Başlıca oyuncular Verizon, AT&T, Vodafone, Deutsche Telekom ve Telefonica gibi şirketleri içerir. Geleneksel olarak, telekomünikasyon şirketleri ITU aracılığıyla uluslararası telekomünikasyon politikasına katılmaktadır. ICANN ve IGF'nin faaliyetlerine giderek daha fazla dahil olmatadırlar. İnternet yönetişimine öncelikli ilgi duymaları, İnternet telekomünikasyon altyapısının daha da geliştirilmesi için işletme dostu uluslararası bir ortam sağlamaktır.

Ek olarak, telekomünikasyon operatörleri, İnternet'ten elde edilen gelirin yeniden dağıtılması sorununu gündeme getirmiştir. İnternete erişim sağladıkları süreç, (reklamcılık temelli gelir getirici modellerinden dolayı şu anda ağırlıklı olarak içerik şirketlerine fayda sağlayan) İnternet kaynaklı gelirin daha yüksek bir kısmını almaları gerektiğini savunmaktadırlar.

İnternet ve telekomünikasyon şirketleri arasında gelirin yeniden paylaşımı ile ilgili tartışma için Bölüm 5'e bakınız.

Telekomünikasyon şirketleri, yeni hizmetler sunarak ve İnternet içerik şirketlerinden daha hızlı hizmet için daha fazla ödeme yapmalarını talep ederek gelirlerini artırmaya çalışmaktadır. Bu tekliflerin birçoğu, ağ tarafsızlık ilkesinin ihlali anlamına gelebilecek, farklı İnternet trafiği türleri için farklı işlemler içermektedir. Bu telekomünikasyon şirketlerini ağ tarafsızlık ilkesinin ana muhaliflerinden birisi yapmaktadır.

Ağ tarafsızlığı konusundaki tartışma için Bölüm 2'ye bakınız.

İnternet gelirin yeniden dağıtılması sorununu ele almaya çalışırken, hem telekomünikasyon şirketleri hem de İnternet endüstrisi birbirlerinin alanlarına girmeye başlamıştır. Telekomünikasyon şirketleri, İnternet içeriği ve iletişim hizmetleri sağlarken, İnternet endüstrisi telekomünikasyon altyapısına yatırım yapmaktadır. Örneğin Google ve Facebook, trans-Atlantik ve trans-Pasifik deniz dibi fiber optik kablolarına yatırım yapmaktadır.

İnternet endüstrisi

İnternet endüstrisi genellikle OTT olarak adlandırılır. İş modeli temelde internete dayanan tüm endüstrileri içerir. İçerik, iletişim ve hizmetler olmak üzere üç ana segmente ayrılırlar. Çoğu büyük şirket birden fazla segmenti kapsamaktadır. Örneğin, Google ve Facebook hem içerik hem de iletişim hizmetleri sunmaktadır.

İnternet İÇERİK endüstrisi

İnternet endüstrisinin çoğu içeriğe dayanır. Google'ın arama motoru çok çeşitli çevrimiçi içeriğe erişim sağlar. YouTube, video materyallerine erişim sağlar. Facebook, kullanıcılar tarafından oluşturulan içeriği düzenler. Disney gibi geleneksel içerik sağlayıcılardan bazıları, başarıyla çevrimiçi içerik sağlayıcılara dönüşmüştür. Bu şirketlerin iş öncelikleri, IPR, mahremiyet, siber güvenlik ve ağ tarafsızlığı gibi çeşitli İnternet yönetimi konularıyla yakından bağlantılıdır. Varlıkları, DTÖ, WIPO ve IGF dahil olmak üzere küresel İnternet yönetim süreçlerinde giderek daha belirgin hale gelmektedir.

İnternet İLETİŞİM endüstrisi

İnternet iletişim hizmetlerindeki en büyük oyuncular Skype, WhatsApp, WeChat, Snapchat ve Google Talk'tur. Bu platformlarda iletişim giderek daha fazla şifrelenmektedir ve genellikle

ulusal hükümetler buna karşı çıkmaktadır. Bu nedenle, İnternet iletişim endüstrisi için ana zorluk, şifreli iletişimin kullanılmasını ve müşterilerinin mahremiyet haklarının korunmasını sağlamaktır.

İnternet SERVİS endüstrisi

İnternet hizmetleri endüstrisi ayrıca bir platform endüstrisi olarak da adlandırılır. Uber ve Airbnb gibi yeni hizmet türlerini içerir. Bu şirketler İnterneti, (Uber tarafından) toplu taşıma araçları için özel araçların kullanımı gibi yeni hizmetler sunmak için kullanmaktadır. Onların işletme modeli, vergilendirme, tüketicinin korunması ve işçi hakları dahil olmak üzere pek çok İnternet yönetişimi sorunuyla yakından bağlantılıdır.

Sivil toplum

Sivil toplum, İnternet yönetimine çok paydaşlı bir yaklaşımın en sesli ve aktif destekçisi olmuştur. Sivil toplum aynı zamanda İnternet yönetim süreçlerinde en çeşitli paydaş grubudur. Sivil toplum grupları, İnternet ile ilgili farklı konulara odaklanmaktadır; çoğu, ifade özgürlüğü ve mahremiyet de dahil olmak üzere, İnternet'teki insan haklarının korunmasının güçlü taraftarlarıdır. Sivil toplum grupları arasındaki en büyük farklardan biri, hükümetlerin İnternet yönetimindeki rolleriyle ilgilidir. Geleneksel olarak, sivil toplum aktörleri, hükümetleri, sivil toplumun, işletmelerin ve teknik topluluğun yanı sıra, İnternet yönetim süreçlerinde diğer eşit katılımcılardan biri olarak görmüştür. Daha yakın zamanlarda, sivil toplum içinde, hükümetlerin meşruiyete dayalı olarak kamu çıkarlarını korumakta lider bir rol oynaması gerektiği yönünde görüşler ortaya koymaya başlamıştır. Özellikle, bu konum, sadece hükümetlerin, dijital sektördeki iş dünyasının çok güçlü rolünü dengeleyebileceği görüşü ile desteklenmektedir.¹⁹

Muhtelif İnternet yönetişimi konularındaki görüş çeşitliliği, uluslararası toplantılarda sivil toplum konumunun koordinasyonunu özellikle zorlaştırmıştır. WSIS sürecinde, sivil toplumun temsili, bu doğal karmaşıklığı ve çeşitliliği bir Sivil Toplum Bürosu, Sivil Toplum Genel Kurulu ve İçerik ve Tema Grubu dahil olmak üzere farklı örgütsel biçimlerde kullanılmaya başlamıştır. WGIG'nin çok paydaşlı olması nedeniyle, sivil toplum bu süreçte üst düzeyde dahil olmuştur. Sivil toplum grupları, daha sonra BM Genel Sekreteri tarafından atanan WGIG için sekiz aday önermiştir. Grubun üyeleri olarak, IGF'yi İnternet yönetişimi konularını tartışmak için çok paydaşlı bir alan olarak belirleme kararı da dahil olmak üzere birçok sonucu etkilemeyi başarmışlardır.

Sivil toplum, IGF faaliyetlerine aktif olarak katılmaya devam etmiştir. İnternet yönetim süreçlerinde sivil toplum temsiline kendine özülüğünün biçimlerinden biri İnternet Yönetişim Grup Toplantısı'dır (IGC). Bir posta listesi biçiminde ele alınan İnternet yönetişimi konularında fikirlerini, politika seçeneklerini ve uzmanlığını paylaşmak isteyen bireyleri içerir.

Sivil toplum kuruluşları esas olarak kamu çıkarlarının korunmasına odaklanarak altyapı gelişiminden ekonomik modellere, hak ve özgürlüklere kadar hemen hemen tüm İnternet yönetişimi konularında etkindir. Birçok kurum sağlam bilgi birikimi ve İnternet spesifikasyonlarını anla-

ma konusunda uzman ve uzman kişiler kullanmakta ve karar verme sürecine değerli katkılar sağlamaktadır.

Sivil toplum örgütlerinin en büyük zorluklarından biri faaliyetlerinin sürdürülebilirliğidir. WSIS sürecinin ilk günlerinde, sivil toplumun katılımının büyük bir kısmı bağlı kişiler etrafında yoğunlaşmıştı. Bu erken dinamizm sağlarken, sivil toplumun sürdürülebilir katılımı için de bir risk oluşturmıştır. Sürdürülebilir sivil toplum katılımı, sürdürülebilir örgütlenmeleri gerektirir. APC, İnternet yönetiminde rol oynayan ilk organizasyon oyuncusu olmuştur. Best Bytes ve Just Net Koalisyonu da sivil toplumun örgütlü girişimleri olarak ortaya çıkmıştır.

Birkaç milyar İnternet kullanıcısı ile İnternet'in sivil toplumu, gerçek toplumun çeşitliliğini ve farklılıklarını yansıtmaktadır. Sivil toplum için asıl zorluk, dijital politikadaki bu görüş çeşitliliği ve konumlarını temsil etmeye devam etmek olarak kalacaktır.

Uluslararası organizasyonlar

ITU, WSIS sürecindeki merkezi uluslararası organizasyon olmuştur. ITU WSIS Sekreteryası'na ev sahipliği yapmış ve ana konular hakkında politika geliştirilmesini sağlamıştır. ITIS'in WSIS sürecine katılımı, giderek artan şekilde İnternet tarafından şekillenen hızlı değişen küresel telekomünikasyon arenasında yeni konumunu tanımlama ve pekiştirme girişiminin bir parçasıydı. ITU'nun rolüne çeşitli şekillerde karşı çıkmıştır. Örneğin, ITU, DTÖ liderliğindeki küresel telekomünikasyon pazarının serbestleştirilmesi nedeniyle geleneksel politika alanını kaybetmektedir. Telefon trafiğini geleneksel telekomünikasyondan İnternete (VoIP üzerinden) taşıma eğilimi, ITU'nun küresel telekomünikasyon alanındaki düzenleyici ayak izini daha da silmektedir.

ITU'nun, fiili Uluslararası İnternet Organizasyonu olarak WSIS sürecinden kaynaklanmış olabileceği ihtimali, bazı gelişmekte olan ülkelerde destek bulurken, ABD ve diğer bazı gelişmiş ülkelerde endişe yaratmıştır. WSIS boyunca, bu olasılık temel politika gerginliklerini ortaya çıkarmıştır. ICANN ile ITU arasındaki gerginliğin 1998'de ICANN'ın kurulmasından bu yana var olduğu İnternet yönetişimi alanında özellikle açıktı. Bu gerginlik WSIS tarafından çözülmedi, ancak daha sonra büyük ölçüde etkisiz hale getirildi. Çeşitli iletişim teknolojilerinin gittikçe artan yaklaşması ile birlikte, ITU'nun İnternet yönetimi alanındaki daha aktif rolü sorusunun küresel politika gündeminde kalması muhtemeldir. Mesela, ITU siber güvenlik ve çevrimiçi çocuk koruma alanında aktif durumdadır.

Diğer bir konu, BM uzmanlık kurumları ailesindeki multidisipliner WSIS gündeminin bağlanması olmuştur. Sosyal, ekonomik ve kültürel özellikler gibi İletişimin ve internet teknolojisinin teknik olmayan yönleri, diğer BM kuruluşlarının görevlerinin bir parçasıdır. Bu bağlamda en öne çıkan oyuncu, çok dillilik, kültürel çeşitlilik, bilgi toplumu ve bilgi paylaşımı gibi konuları ele alan UNESCO'dur. WIPO ayrıca, IPR'nin dijital alanda korunması ile ilgili konularda İnternet yönetim tartışmalarında aktif olarak yer almaktadır.

ITU ile diğer BM kuruluşları arasındaki denge dikkatlice yönetilmiştir. WSIS izleme süreçleri, ITU'nun koordinasyon rolü ve UNESCO, UNDP ve UNCTAD'ın katılımıyla da bu dengeyi

yansıtmaktadır. Örneğin, bu Birleşmiş Milletler ajansları, son birkaç yılda İnternet yönetişimi ile ilgili konularda daha fazla tartışmayı içeren yıllık WSIS Forumunun ana düzenleyicileri olmuşlardır.

Teknik toplum

Teknik topluluk, İnternet'in geliştirilmesine katılan ve/veya İnternet teknik kaynaklarını yöneten kurumları ve bireyleri içerir. Teknik topluluk ayrıca, kaynakları paylaşma, açık erişim ve İnternet düzenlemesine devletin dahil olmasına karşı çıkma ilkelerine dayanarak İnternetin ilk ruhunu yaratmıştır. Üyeleri, başından beri, İnternetin ilk konseptini yoğun ticarileşmeden ve kapsamlı devlet etkisinden korumuşlardır.

Terminoloji: Teknik toplum

Diğer terimler, İnternet topluluğu, İnternet geliştiricileri, İnternet kurucuları, İnternet babaları ve teknoloji uzmanları gibi “teknik topluluk” ile değiştirilerek kullanılır. “Teknik topluluk” terimi, WSIS bildirimlerinde ve diğer politika belgelerinde kullanılmaktadır.

Teknik topluluk, Peter Haas'ın ‘aynı sebep-sonuç ilişkilerine inanan, gerçekleri kabul etmek için onları test eden ve problemleri anlama ve çözme konusunda ortak değerleri paylaşan profesyonel bir grup’ olarak tanımladığı²⁰ epistemik (bilgiyle uğraşan) bir topluluğun tüm kriterlerini yerine getirmektedir.

İlk teknik topluluk, RFC'ler olmak üzere, birkaç tane temel davranış, kural ve temel bir resmi prosedürle koordine edilmiştir. İnternetin tüm ana ve temel standartları RFC'ler aracılığıyla tanımlanmaktadır. Sıkı bir düzenlemeye veya resmi bir yapıya sahip olmasa da, ilk İnternet topluluğu güçlü gelenekler ve eşitler arasındaki normlarla yönetiliyordu. Bu süreçteki çoğu katılımcı benzer değerleri, takdir sistemlerini ve tutumlarını paylaşmıştır.

İnternetin en başında teknik topluluk tarafından yönetilmesi, İnternet'in küresel sosyal ve ekonomik yaşamın bir parçası haline gelmesinden sonra 1990'ların ortalarında muhalefet ile karşılaşmıştır. İnternetin büyümesi, iş dünyası gibi farklı meslek kültürleriyle birlikte, İnternet ve onun yönetişimini anlama ile gelen ve artan gerilime yol açan bir grup yeni paydaş ortaya çıkarmıştır. Örneğin, 1990'larda, İnternet topluluğu ve Ağ Çözümleri adlı şirket,²¹ kök sunucunun ve alan adı sisteminin kontrolü üzerinde bir kontrol sağlama çatışması olan sözde DNS savaşına dahil olmuştur.

İnternet Topluluğu, teknik topluluğun ana temsilcilerinden biridir. IETF'e ev sahipliği yapar, açık bir İnterneti savunur ve kapasite geliştirmede aktif rol oynar.

Teknik topluluk, ICANN'ın kurulması ve işletilmesi sürecinde önemli bir aktör olmuştur. İnternetin babalarından biri olan Vint Cerf, 2000'den 2007'ye kadar ICANN Kurulu Başkanıydı. Teknik topluluğun üyeleri, çeşitli ICANN karar organlarında önemli pozisyonlara sahip olmuştur.

Günümüzde, üç milyardan fazla kullanıcısı olan İnternet, ana topluluk olarak teknik topluma odaklanan ilk ICANN tabanlı politika çerçevesinin ötesinde büyümüştür. Bu argümanın ardın-

dan, vatandaşlar ve İnternet kullanıcıları arasındaki çizgi bulanıklaştığından, (teknik toplumun tanımlandığı gibi) sadece İnternet kullanıcılarını temsil edenleri değil, hükümetlerin ve vatandaşları temsil eden diğer yapıların internet yönetişimine daha fazla katılımı gerekmektedir. İnternet yönetişimine daha fazla devlet müdahalesinde bulunmak isteyenler, İnternet kullanıcıları ve toplulukları yerine vatandaşları temsil etmek için bu yaklaşımı kullanmaktadır.

Teknik topluluk genellikle belirli İnternet yönetim süreçlerindeki özel konumunu teknik uzmanlığı ile haklı çıkarmıştır. Örneğin, teknik topluluk ICANN'ın esas olarak teknik bir organizasyon olduğunu ve bu nedenle teknik bilgiyi kullanan teknik kişilerin çalıştırması gerektiğini savunuyordu. ICANN'ı yalnızca teknik bir organizasyon olarak sürdürmenin artan zorluğu ile teknik topluluğun özel rolünün bu gerekçesi sıkça tepki ile karşılaşmıştır. Teknik topluluğun üyelerinin kademeli olarak başta sivil toplum, iş dünyası ve akademi olmak üzere diğer paydaş gruplarına ve ayrıca hükümetlere dahil olması muhtemeldir.

ICANN

ICANN, 1998 yılında ABD merkezli, kar amacı gütmeyen bir şirket olarak kurulmuş ve ABD hükümeti tarafından IP adresleri, etki alanı adları ve kök sunucular hususundaki IANA işlevlerini yerine getirme görevini yapmıştır.

ICANN rolüne artan ilgi, 2000'li yılların başlarında ve İnternet'in hızlı büyümesine paralel olarak gelişmiş ve ICANN, WSIS sürecinde küresel politika çevrelerinin dikkatini çekmiştir (2003-2005).

ICANN'nin şu anki misyonu, 2016'nın gözden geçirilmiş yönetmeliklerine yansıtıldığı gibi, İnternet'in benzersiz tanımlayıcı sistemlerinin istikrarlı ve güvenli bir şekilde çalışmasını sağlamaktır. Bu amaçla, kuruluş DNS kök bölgesinde isimlerin tahsis edilmesi ve atanması ile gTLD'lere ilişkin politikaların geliştirilmesi ve uygulanmasını koordine eder; DNS kök adı sunucu sisteminin koordinasyonunu kolaylaştırır; ve IP numaralarının ve özerk sistem numaralarının genel tahsisini ve atanmasını koordine eder.

ICANN, İnternet yönetişimi alanındaki ana aktörlerden biri olmasına rağmen, İnternet'in tüm yönlerini yönetmemektedir. Bazen, yanlış olsa da, İnternet hükümeti olarak tanımlanmıştır. ICANN İnternet teknik kaynaklarını yönetir, ancak siber güvenlik, içerik politikası, telif hakkı koruması, mahremiyetin korunması, kültürel çeşitliliğin korunması veya dijital uçurumun kapatılması gibi diğer İnternet yönetişimi konularında doğrudan yetkisi yoktur.

ICANN, farklı kapasite ve rollerde çok çeşitli aktörleri içeren çok paydaşlı bir kurumdur. Paydaşlar üç ana gruba ayrılırlar.

- ICANN sistemi içerisindeki rolü, kuruluşun misyonuyla ilgili alanları kapsayan (gTLD'ler, DNS'in güvenliği ve istikrarı gibi) politikalar hakkında ICANN Kuruluna öneriler geliştirmek olan **teknik ve iş dünyası toplulukları**.
- WSIS sürecine başlayan, ICANN'de daha önemli bir role sahip olma konusundaki artan ilgileri ile **ulusal hükümetler**. ICANN'in politika geliştirme süreci çerçevesinde, hükümetle-

rin bir tavsiye rolü bulunmaktadır. ICANN Kuruluna, özellikle kamu politikalarını etkileyecek konularda tavsiyelerde bulunmaktadır.

- Politika geliştirme sürecine katkısı da tavsiye niteliğinde olan **İnternet kullanıcıları** (genel olarak topluluk).

İnternet kullanıcılarının dahil edilmesi

ICANN, İnternet kullanıcılarının dahil edilmesine yönelik çeşitli yaklaşımlar denemiştir. İlk günlerinde ilk girişim, İnternet kullanıcılarını ICANN yönetim organlarına doğrudan temsilci seçimleri yoluyla dahil etmekti. Bu ICANN'ın meşruiyetini koruma girişimiydi. Katılımın azalması ve sürecin kötüye kullanılması nedeniyle doğrudan oylama başarısız olmuştur. Bu İnternet kullanıcılarının gerçek bir temsilini sağlamamıştır. Daha sonra, ICANN, İnternet kullanıcılarını 'büyük' bir yönetim yapısı (Büyük Danışma Komitesi - ALAC) içerisinde, halkla istişareler ve kitlesel kaynak kullanımı yoluyla dahil etmeye başlamıştır.²² Bu örgütsel deneyler ICANN'ın meşruiyetini sağlamak için şart olmuştur.

ICANN'ın karar alma süreci, aşağıdan yukarıya, şeffaf, açık ve kapsayıcı yaklaşımlara dayanan ilk İnternet yönetim süreçlerinden etkilenmiştir. 1980'lerin ilk teknik topluluğu ile mevcut ICANN karar verme bağlamı arasındaki temel farklardan biri 'sosyal sermaye' düzeyidir. Geçmişte, teknik topluluk karar alma ve uyuşmazlık çözümünü şimdi olduğundan çok daha kolay hale getiren karşılıklı güven ve dayanışma seviyelerine sahipti. İnternetin büyümesi, teknik topluluğun çok ötesinde, milyarlarca yeni kullanıcıya ve yeni paydaşlara ulaştı. Sonuç olarak, İnternetin bu hızlı büyümesi, ilk günlerinde var olan sosyal sermayeyi azaltmıştır. Bu nedenle, teknik topluluğun daha önceki, resmi olmayan, karar alma sürecini İnternet'te tutma konusundaki önerileri gerçekçi olmamıştır. Sosyal sermaye olmadan, tamamen işlevsel bir karar alma sürecinin sağlanmasının ana yolu, onu biçimlendirmek ve fren-denge mekanizmaları geliştirmektir.

Karar alma prosedürlerinde bazı düzeltmeler olmuş ve bu değişen gerçeği yansıtacak şekilde yapılmıştır. Örneğin, 2002 ICANN reformu GAC'in güçlendirilmesini ve İnternet kullanıcıları için doğrudan oylama sisteminin terk edilmesini içeriyordu. ICANN'ın küresel İnternet topluluğuna karşı hesap verebilirliğini artırmak amacıyla şu anda daha fazla değişiklik yapılmaktadır.

Meseleler

Politika yönetimine karşı teknik yönetim

Teknik ve politika yönetimi arasındaki ikilim, ICANN'ın faaliyetlerinde sürekli bir gerilim yaratmıştır. ICANN, kendisini yalnızca teknik meselelerle ilgilenen ve İnternetin kamu politikalarından uzak kalan İnternet için teknik bir koordinasyon organı olarak resmetmiştir. ICANN yetkilileri, bu spesifik teknik yapıyı, kurumun benzersiz statüsünü ve örgütsel yapısını savunmak için temel kavramsal argüman olarak değerlendirmiştir. ICANN'ın ilk başkanı Esther Dyson şunları vurguladı: 'ICANN, herhangi bir İnternet yönetişimi sorununu "ele almak istemedi"; aslında, ICANN insanları değil sıhhi tesisatı yönetmektedir. Genel olarak İnternet altyapısının ve özellikle Alan Adı Sisteminin belirli (büyük ölçüde teknik) yönlerini yönetmek için çok sınırlı bir yetkiye sahiptir.'²³

Bu iddianın eleştirmenleri genellikle teknik olarak nötr bir çözüm bulunmadığına işaret eder. Sonuçta, her teknik çözüm veya karar belirli çıkarları teşvik eder, belirli gruplara güç verir ve sosyal, politik ve ekonomik hayatı etkiler. .xxx TLD ve 2014'te tanıtılan yeni gTLD'ler gibi konularla ilgilenmek, ICANN'ın teknik meselelerin kamu politikası yönleri ile ilgilenmesi gerektiği gerçeğini giderek daha fazla göstermektedir.

Yönetimin IANA geçişi ve ICANN'ın hesap verebilirliği

ICANN, 1 Ekim 2016 tarihine kadar IANA işlevlerini ABD hükümetiyle (NTIA aracılığıyla Ticaret Bakanlığı ile) yapılan bir sözleşme temelinde gerçekleştirmiştir. Bu sözleşme uyarınca, ABD hükümeti, (ICANN bazı yeni gTLD'leri onaylamaya karar verdiğinde, bu tür kararların her biri için ABD hükümetinin resmi onayını gerektirmesi gibi) DNS içinde yapılan her büyük değişiklik konusunda nihai yetkiye sahipti.

ABD hükümeti Mart 2014'te, IANA fonksiyonları üzerindeki yönetim rolünü küresel çok paydaşlı topluluğa geçirmek istediğini açıkladı.²⁴ ICANN'den bir geçiş teklifinin geliştirilmesi için bir süreç başlatması istendi. Aynı zamanda, ICANN'ın hesap verebilirlik mekanizmalarını geliştirmek için bir dizi öneri hazırlanmasına yönelik çalışmalar başladı. ICANN topluluğu, 2014 ve 2016 yılları arasında, Mart 2016'da ICANN Kurulu tarafından onaylanan ve ABD hükümeti tarafından Haziran 2016'da gereklilikleri uyarınca kabul edilen geçiş ve hesap verebilirlik tekliflerinin hazırlanmasında yoğun bir şekilde çalışmıştır.

IANA yönetim geçiş önerisi doğrultusunda, ICANN ile yapılan sözleşmeye dayanarak IANA adlandırma işlev operatörü olan bir alt şirket olarak PTI'yi kurdu. Bu, alanı adları ile ilgili IANA işlevlerinin ICANN çerçevesiyle yapılmaya devam ettiği, ancak teknik işlevlerle ICANN'ın politika oluşturma işlevleri arasında daha net bir ayrım olduğu anlamına gelmektedir. 1 Ekim 2016'da yürürlüğe giren gözden geçirilmiş ICANN düzenlemeleri, bir inceleme sürecinin IANA fonksiyon operatörlerinin ICANN'den ayrılmasına neden olabileceği koşulunun altını çizdi. Daha önce ABD hükümetinin resmi onayına tabi olan DNS kök bölgesindeki önemli değişiklikler şimdi ICANN Yönetim Kurulu tarafından onaylanmaya tabi hale gelmiştir.

IP numaraları ve protokol parametreleri ile ilgili IANA fonksiyonlarının performansı da PTI'ye verilmiştir. Bu işlevlerin yerine getirilmesine ilişkin anlaşmalar, ICANN ve (IP adreslerinin bölgesel olarak tahsisi ve yönetiminden sorumlu olan RIR'ler olan) numaralandırma kaynakları topluluğu ve (IETF ve IAB tarafından temsil edilen) protokol parametreleri topluluğu arasında belirlenmiş ve ardından ICANN ile PTI arasında alt sözleşmeler yapılmıştır.

ICANN'ın daha geniş bir İnternet topluluğuna karşı hesap verebilirliği ile ilgili olarak, ABD hükümetinin yönetim rolünün ortadan kalkması ile, kuruluş içinde yeni mekanizmalar uygulamaya konmuştur. Bunlardan en önemlisi, ICANN Kurulunun üyelerini azletmek, ICANN bütçelerini reddetmek ya da ICANN düzenlemelerindeki değişiklikleri reddetmek gibi bir dizi topluluk yetkisini uygulama yeteneğine sahip olan ve ortak olmayan bir dernek olarak işlev gören yeni bir tüzel kişiliğin (**güçlendirilmiş topluluk**) oluşturulmasıdır. Bu tüzel kişilik, karar veren ICANN'ın danışma komiteleri ve İnternet kullanıcılarını temsil eden kurumlar, hükümetler, özel sektör ve teknik topluluktan oluşan çoğu katılımcıların belirttiği şekilde hareket etmektedir.²⁵

Son notlar

- 1 Ülke alan adının yönetiminin Brezilya modeli genellikle çok paydaşlı yaklaşımın başarılı bir örneği olarak kabul edilir. Brezilya etki alanlarından sorumlu ulusal organ - CGI - devlet yetkilileri, iş sektörü ve sivil toplum dahil olmak üzere tüm kullanıcılara açıktır. Brezilya, özellikle Rio de Janeiro ve João Pessoa'da düzenlenen IGF 2007 ve 2014 hazırlık süreci sürecinde, bu modeli yavaş yavaş İnternet yönetiminin diğer alanlarına genişletti. Brezilya İnternet yönetiminde, özellikle Brezilya Cumhurbaşkanı Dilma Rousseff ve ICANN Başkanı Fadi Chehadé tarafından başlatılan bir süreç olan NetMundial'de (<http://netmundial.br>) aktif olmaya devam etti. NetMundial Girişimi (<https://www.netmundial.org/>).
- 2 Ulusal IGF girişimlerinin güncellenmiş bir listesi için bkz. Internet Governance Forum (no date) National IGF initiatives. <http://www.intgovforum.org/multilingual/content/national-igf-initiatives> [Erişim 6 Kasım 2016]. The IGF website also includes a list of recognised regional IGF initiatives: Internet Governance Forum (no date) Regional IGF initiatives. Avail- able at <http://www.intgovforum.org/multilingual/content/regional-igf-initiatives> [Erişim 6 Kasım 2016].
- 3 Géraud A (1954) The rise and fall of the Anglo-French Entente. Foreign Affairs. <http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente> [Erişim 29 Ekim 2016].
- 4 Lesage C (1915) La rivalite franco-britannique. Les cables sous-marins allemands Paris. p. 257-258; quoted in: Headrick D (1991) The Invisible Weapon: Telecommunications and International Politics 1851-1945. Oxford: Oxford University Press. p. 110.
- 5 Mueller M (1999) ICANN and internet governance: Sorting through the debris of 'self-regulation'. info (The Journal of Policy, Regulation and Strategy for Telecommunications Information and Media) 1(6), p 497-520. http://www.icannwatch.org/archive/mueller_icann_and_internet_governance.pdf [Erişim 14 March 2016].
- 6 ABD Dışişleri Bakanı, ITU'yu inisiyatif için şu şekilde eleştirmektedir: 'Üye hükümetlerin yetkilendirmesi olmayan bir kaynak harcaması ve uluslararası anlaşmalar içeren bir toplantı yapmak.' Bkz. Drake W (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. <http://www.un-ngls.org/orf/drake.pdf> [Erişim 29 Ekim 2016].
- 7 Internet World Stats (2015) Internet Usage in the European Union. <http://www.internetworldstats.com/stats9.htm> [Erişim 14 Kasım 2016].
- 8 European Commission (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. European Commission – IP/13/371. http://europa.eu/rapid/press-release_IP-13-371_en.htm [Erişim 29 Ekim 2016].
- 9 Alibaba Group (no date) Electronic World Trade Platform. <http://www.alizila.com/wp-content/uploads/2016/09/eWTP.pdf> [Erişim 12 Kasım 2016].
- 10 Ministry of Foreign Affairs of the People's Republic of China (2015) Remarks by H.E. Xi Jinping, President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [Erişim 12 Kasım 2016].
- 11 Rousseff D (2013) Statement by H.E. Dilma Rousseff, president of the Federative Republic of Brazil, at the opening of the general debate of the 68th Session of the United Nations General Assembly. https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [Erişim 29 Ekim 2016].

- 12 NETmundial (2014) NETmundial Multistakeholder Statement. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> [Erişim 29 Ekim 2016].
- 13 Goldstein D (2016) Indian Minister of Electronics and Information Technology Reaffirms Support of the Multistakeholder Model at ICANN's 57th Public Meeting. Domain Pulse, 6 Kasım. <http://www.domainpulse.com/2016/11/06/india-reaffirms-support-multistakeholder-model-icann57/> [Erişim 6 Kasım 2016].
- 14 United Nations General Assembly (1999) Resolution A/53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [Erişim 8 Kasım 2016].
- 15 Radu R (2013) Negotiating meanings for security in the cyberspace. Info 15(6), pp. 32–41. Available at https://www.researchgate.net/publication/255697155_Negotiating_meanings_for_security_in_the_cyberspace [Erişim 14 March 2016].
- 16 The convenience of 'one-stop shopping' was one of the arguments for establishing the ITU as the central Internet governance player.
- 17 WSIS (2003) Declaration of principles. <http://www.itu.int/wsis/docs/geneva/official/dop.html> [Erişim 12 Kasım 2016].
- 18 Değerli yorumlar Ayesha Hassan tarafından sağlandı.
- 19 Bu görüş, özellikle Just Net Koalisyonu tarafından desteklenmiştir ve kuruluş tarafından yayınlanan çeşitli beyanlara ve beyanlara yansıtılmıştır. Detaylar için bkz. Just Net Coalition (no date) Statements. <http://justnetcoalition.org/statements> [Erişim 10 Kasım 2016].
- 20 Haas P (1990) Saving the Mediterranean: The Politics of International Environmental Cooperation. New York: Columbia University Press, p.55
- 21 Teknoloji şirketi Network Solutions www.networksolutions.com, 1979 yılında kuruldu. Alan adı tescilli işi, şirketin en önemli bölümü idi; Şirket portföyünü küçük işletmeler için web hizmetleri içerecek şekilde çeşitlendirdi.
- 22 Radu R et al. (2015) Crowdsourcing ideas as an emerging form of multistakeholder participation in Internet governance. Policy & Internet 7(3), pp. 362–382
- 23 Dyson E (1999) Esther Dyson's response to Ralph Nader's Questions. <http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm> [Erişim 14 March 2016].
- 24 NTIA (2014) NTIA Announces Intent to Transition Key Internet Domain Name Functions. <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions> [Erişim 29 Ekim 2016].
- 25 IANA yönetim geçişi ve ICANN hesap verebilirlik süreçleri hakkında daha fazla bilgi için bkz. GIP Digital Watch observatory (no date) IANA Transition and ICANN Accountability. <http://digitalwatch.giplatform.org/processes/iana> [Erişim 29 Ekim 2016].

DIPLO

DiploFoundation, diplomasiyi ve uluslararası yönetişimi daha kapsayıcı ve etkili hale getirmeye yönelik kar amacı gütmeyen bir kuruluştur. Diplo, özellikle şunlar için çalışmaktadır:

- Küçük ve gelişmekte olan devletlerin uluslararası ilişkilere anlamlı bir şekilde katılmalarını sağlamak.
- Uluslararası hesap verebilirliği ve kapsayıcılığı arttırmak için.
- Uluslararası politika sürecinin meşruiyetini artırmak.
- Küresel yönetişimi ve uluslararası politika geliştirme sürecini iyileştirmek.

Diplo'nun temel faaliyetleri:

Kapasite geliştirme: Diplo'nun kapasite geliştirme desteği bireylerle başlar, ancak etkimiz bu bireylerin faaliyetleri aracılığıyla onların ve kuruluşlarının parçası olduğu daha büyük sistemlere ulaşır. Yaklaşımımız, çevrimiçi eğitim, politika araştırması, politikaya katma ve her politika bağlamına uygun olarak çeşitli şekillerde bir araya getirilmiş uygulama topluluklarının geliştirilmesini içerir. Kapasite geliştirme konuları arasında İnternet yönetimi, e-diplomasi, kamu diplomasisi, insani diplomasi ve küresel sağlık diplomasisi yer almaktadır.

Etkinlikler: Küresel yönetimdeki acil sorunların üstesinden gelmek için etkinliklerimiz, diplomatlar, iş dünyası çalışanları ve sivil toplum üyeleri de dahil olmak üzere insanları farklı bakış açılarıyla bir araya getiriyor. Uzaktan katılımı destekleyen e-araçlar yoluyla etkinliklerimizi daha erişilebilir hale getirmek için çalışıyoruz. Etkinliklerimiz genellikle eğitim faaliyetlerine, yayınlara veya çevrimiçi etkileşime dönüşüyor.

Kurslar: Diplomatlar, memurlar, uluslararası kuruluşlar ve STK'lar ve Uluslararası İlişkiler öğrencileri için yüksek lisans düzeyinde akademik kurslar ve çeşitli diplomasi ile ilgili konularda eğitim atölyeleri sunuyoruz. Çok gelişmiş bir öğrenme metodolojisini benzersiz çevrimiçi öğrenme platformumuzla birleştiren kurslarımız esnek, kişisel, etkileşimli ve topluluk oluşturmaktadır. Kurslar çevrimiçi olarak, yüz yüze ve karma biçimde sunulmaktadır.

Araştırma: Kitle kaynak kullanımı, trend analizi ve işbirliğine dayalı araştırma gibi İnternet tabanlı tekniklerle geleneksel politika araştırma yöntemlerini geliştiriyoruz. Konular diplomasi, İnternet yönetimi ve çevrimiçi öğrenmeyi içermektedir.

Yayınlar: Yayınlarımız diplomasi alanındaki güncel gelişmelerin incelenmesinden geleneksel yönleriyle ilgili yeni analizlere kadar uzanmaktadır. Yayınlarımızın birçoğu, çevrimiçi olarak ve basılı formatta mevcuttur ve bazıları birçok dile çevrilmiştir.

2002 yılında Malta ve İsviçre hükümetleri tarafından kurulmuş ve Msida, Malta, Cenevre, İsviçre, Belgrad ve Sırbistan'da ofisleri bulunmaktadır. Diplo 2006'dan bu yana UN ECOSOC nezdinde danışman statüsündedir.

Diplo hakkında daha fazla bilgi için, bkz. <https://www.diplomacy.edu>

Cenevre İnternet Platformu

İsviçre Federal Dışişleri Bakanlığı (EDA) ve Federal İletişim Ofisi (OFCOM), bir gözlemevi, kapasite oluşturma ve tartışma merkezi görevlerini (çevrimiçi ve yerinde) yerine getiren **Cenevre İnternet Platformu**'nu (GIP) gündeme getirmiştir. GIP, İsviçre makamları tarafından desteklenen ve DiploFoundation tarafından işletilen bir girişimdir.

GIP'in faaliyetleri üç ayağa dayanarak uygulanmaktadır:

- Cenevre'deki fiziksel platform
- Çevrimiçi platform ve gözlemevi
- Yenilik labaruarı

GIP'in özel odağı, küçük ve gelişmekte olan ülkelere İnternet yönetim süreçlerine anlamlı bir şekilde katılmaları konusunda yardım etmektir. Destek, eğitim, bilinçlendirme, istişareler ve brifingler dahil olmak üzere bu aktörlerin ihtiyaçlarına göre düzenlenmiştir.

GIP faaliyetleri hakkında daha fazla bilgi için, bkz. <http://www.giplatform.org>

DigitalWatch

GIP Dijital Watch, İnternet yönetiřimi ve dijital politika uygulayıcılarına devam eden gelişmeler hakkındaki güncel bilgilerden haberdar olmalarını sağlayan bir araç sağlamayı amaçlamaktadır. GIP Digital Watch, DiploFounda'nın son 20 yılda geliřtirdiđi materyallere, bilgi yönetimi uzmanlığına ve ađlara dayanmaktadır.

GIP Digital Watch inisiyatifiinin üç ayađı bulunmaktadır:

GIP Dijital Watch gözlemevi, İnternet yönetiřimi ve dijital politika ile ilgili canlı gelişmeler, genel bakışlar ve açıklayıcı metinler, etkinlikler, kaynaklar ve diđer içerikler için tarafsız bir tek durak imkanı sunmaktadır.

Aylık bir bülten olan Cenevre Dijital Saat bülteni, bir dizi gelişmeyi, önde gelen uzmanlarla röportajları ve çeřitli dijital politika alanlarındaki makaleleri içerir.

Cenevre'de İnternet üzerinden ve İnternette aylık olarak yapılan internet yönetiřimi GIP briefingleri her ayın son salı günü gerçekleşmektedir. 2016 itibariyle, yerel topluluklarda sürdürülebilir tartışmaları teşvik etmek ve aylık briefingler sırasında bölgesel perspektifleri paylaşmak için dünya çapında yerel merkezler kurulmaktadır.

GIP Digital Watch hakkında daha fazla bilgi için, bkz. <https://digitalwatch.giplatform.org>

SÖZLÜK

3G	third-generation mobile networks	Üçüncü Nesil Mobil Ağlar
4G	fourth-generation mobile networks	Dördüncü Nesil Mobil Ağlar
5G	fifth-generation mobile networks	Beşinci Nesil Mobil Ağlar
ACTA	Anti-Counterfeiting Trade Agreement	Sahteciliğe Karşı Ticaret Anlaşması
ADA	Azerbaijan Diplomatic Academy	Azərbaycan Diplomatik Akademisi
ADR	Alternative Dispute Resolution	Alternatif Uyuşmazlık Çözümü
AFRINIC	African Network Information Centre	Afrika Ağ Bilgi Merkezi
AFTLD	Africa Top Level Domains Organization	Afrika Üst Düzey Alan Adı Teşkilatı
AI	artificial intelligence	Yapay Zeka
ALAC	At-Large Advisory Committee (ICANN)	Genişletilmiş Danışma Komitesi
APEC	Asia-Pacific Economic Cooperation	Asya Pasifik İşbirliği
APC	Association for Progressive Communications	İletişimi Geliştirme Birliği
APNIC	Asia Pacific Network Information Centre	Asya Pasifik Ağ Bilgi Merkezi
APTLD	Asia Pacific Top Level Domain Association	Asya Pasifik Üst Düzey Alan Adı Birliği
ARPAnet	Advanced Research Projects Agency Network	İleri Araştırma Projeleri Ajansı Bilgisayar Ağı
ARF	Association of Southeast Asian Nations (ASEAN) Regional Forum	Güneydoğu Asya Ulusları Bölgesel Forumu Birliği (ASEAN)
ARIN	American Registry for Internet Numbers	Amerika İnternet Numaraları Kütüğü
ASCII	American Standard Code for Information Interchange	Bilgi Değişimi Amaçlı Amerikan Standart Kodlama Sistemi
ASEAN	Association of Southeast Asian Nations	Güneydoğu Asya Ulusları Birliği
AU	African Union	Afrika Birliği
AXIS	African Internet eXchange System (AU)	Afrika İnternet Değişimi Sistemi (AB)
BEREC	Body of European Regulators for Electronic Communications	Avrupa Elektronik İletişim Düzenleyiciler Kurumu
BIS	Bank for International Settlements	Uluslararası İskan Bankası
BGPsec	Border Gateway Protocol Security	Sınır Ağ Geçidi Protokolü Güvenliği
BRICS	Brazil, Russia, India, China, and South Africa	Brezilya, Rusya, Hindistan, Çin ve Güney Afrika
BTA	Basic Telecommunication Agreement	Temel Telekomünikasyon Anlaşması
CA	Certificate Authority	Sertifika Yetkilisi
CBMs	confidence-building measures	Güven Artırıcı Önlemler
CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO)	Kooperatif Siber Savunma Mükemmeliyet Merkezi (NATO)
ccNSO	Country Code Names Supporting Organization (ICANN)	Ülke Kodu İsimleri Destekleme Teşkilatı (ICANN)
ccTLD	country code top-level domain	Ülke Kodu Üst Düzey Alan İsimleri
CDNs	content delivery networks	İçerik iletilen ağlar
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women (UN)	Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşmesi (BM)
CEFACT	Centre for Trade Facilitation and Electronic Business (UN)	Ticaretin Kolaylaştırılması ve Elektronik Ticaret Merkezi
CEN	European Committee for Standardization	Avrupa Standartlaştırma Komitesi
CENTR	Council of European National Top Level Domain Registries	Avrupa Ulusal Üst Düzey Alan Adları Kütükleri Konseyi
CERN	European Organization for Nuclear Research	Avrupa Nükleer Araştırma Teşkilatı
CEO	Chief Executive Officer	Baş Yönetici
CERT	Computer Emergency Response Team	Bilgisayar Acil Durum Müdahale Ekibi
CGI.br	Brazilian Internet Steering Committee	Brezilya İnternet Yönlendirme Komitesi

CI	critical infrastructure	Kritik Altyapı
CIA	confidentiality, integrity, availability	Mahremiyet, Bütünlük, Mevcudiyet
CICTE	Inter-American Committee against Terrorism	Amerikalılar Arası Terörizmle Mücadele Komitesi
CIDR	Classless Inter-Domain Routing	Sınıfsız Alan Adları Arası Yönlendirme
CIGF	Commonwealth Internet Governance Forum	İngiliz Milletler Topluluğu İnternet Yönetişimi Forumu
CII	critical information infrastructure	Kritik Bilgi Alt Yapısı
CIIP	critical information infrastructure protection	Kritik Bilgi Alt Yapısının Korunması
CIR	critical Internet resources	Kritik İnternet Kaynakları
CITEL	Inter-American Telecommunication Commission	Amerikalılar Arası Telekomünikasyon Komisyonu
CJEU	Court of Justice of the European Union	Avrupa Birliği Adalet Divanı
CND	content delivery networks	İçerik Dağıtım Ağları
CoE	Council of Europe	Avrupa Konseyi
COMESA	Common Market for Eastern and Southern Africa	Doğu ve Güneydoğu Afrika İçin Ortak Pazar
COP	Child Online Protection (ITU initiative)	Çocukların Çevrim İçi Korunması (ITU İnisiyatifi)
CRC	Convention on the Rights of the Child (UN)	Çocuk Hakları Sözleşmesi (BM)
CRPD	Convention on the Rights of Persons with Disabilities (UN)	Engellilerin Hakları Sözleşmesi (BM)
CSIRT	Computer Security Incident Response Team	Bilgisayar Güvenliği Olay Müdahale Ekibi
CSS	cascading style sheets	Basamaklı Stil Şablonu
CSTD	Commission on Science and Technology for Development (UN)	Kalkınma için Bilim ve Teknoloji Komisyonu (BM)
DDoS	distributed denial of service	Hizmetin Dağıtılmış Reddi
DMCA	Digital Millennium Copyright Act (USA)	ABD'nin Dijital Milenyum Telif Hakkı Yasası
DNS	Domain Name System	Alan Adı Sistemi
DNSSEC	Domain Name System Security Extensions	Alan Adı Sistemi Güvenlik Uzatıları
DOA	Digital Object Architecture	Dijital Nesne Mimarisi
DoS	denial of service	Hizmet Reddi
DSL	digital subscriber line	Dijital Abone Hattı
DWDM	dense wavelength division multiplexing	Yoğun Dalga Boyu Bölmeli Çoğullama
ebXML	electronic business XML	Elektronik İşletme XML
ECHR	European Court of Human Rights	Avrupa İnsan Hakları Mahkemesi
ECOSOC	Economic and Social Council (UN)	Ekonomik ve Sosyal Konsey (BM)
ECTS	European Credit Transfer and Accumulation System	Avrupa Kredi Transferi ve Biriktirme Sistemi
EDI	electronic data interchange	Elektronik Veri Değişimi
eIDAS	Regulation on electronic identification and trust services for electronic transactions in the internal market (EU)	İç Pazardaki Elektronik İşlemlerde Elektronik Kimlik Ve Güven Hizmetleri Yönetmeliği
ENISA	European Union Agency for Network and Information Security	Ağ ve Bilgi Güvenliği için Avrupa Birliği Ajansı
EPC	electronic product code	Elektronik Ürün Kodu
EPCIP	European Programme for Critical Infrastructure Protection	Avrupa Kritik Alt Yapı Koruma Programı
ETNO	European Telecommunications Network Operators	Avrupa Telekomünikasyon Ağ Operatörleri
ETSI	European Telecommunications Standards Institute	Avrupa Telekomünikasyon Standartları Birliği
EuroDIG	European Dialogue on Internet Governance	İnternet Yönetişiminde Avrupa Diyalogu
EuroISPA	European Internet Service Providers Association	Avrupa İnternet Hizmet Sağlayıcıları Birliği
Europol	European Police Office	Avrupa Polis Ofisi

FATF	Financial Action Task Force	Mali Eylem Görev Gücü
FBI	Federal Bureau of Investigation (USA)	Federal Soruşturma Bürosu (ABD)
FCC	Federal Communications Commission (USA)	Federal İletişim Komisyonu (ABD)
FIRST	Forum of Incident Response and Security Teams	Olaya Müdahale ve Güvenlik Ekipleri Forumu
GAC	Governmental Advisory Committee (ICANN)	Hükümet Tavsiye komitesi (ICANN)
GATS	General Agreement on Trade in Services	Hizmet Ticareti ile İlgili Genel Anlaşma
GATT	General Agreement on Tariffs and Trade	Gümrük Tarifeleri ve Ticaret Genel Anlaşması
GCA	Global Cybersecurity Agenda	Küresel Siber Güvenlik Ajandası
GCCS	Global Conference on CyberSpace	Siber Alanda Küresel Konferans
GCI	Global Cybersecurity Index	Küresel Siber Güvenlik Endeksi
GFCE	Global Forum on Cyber Expertise	Siber Uzmanlık Küresel Forumu
GIP	Geneva Internet Platform	Cenevre İnternet Platformu
GICGM	High-Level Panel on Global Internet Cooperation and Governance Mechanisms	Küresel İnternet İşbirliği ve Yönetişim Mekanizmaları
GSM	Global System for Mobile Communications	Mobil İletişim için Küresel Sistem
GSMA	Groupe Speciale Mobile Association	Özel Grup Mobil Birliği
gTLD	generic top-level domain	Jenerik Üst Düzey Alan Adları
HD	high definition	Yüksek Çözünürlük
HTCIA	High Technology Crime Investigation Association	Yüksek Teknoloji Suçlarını Araştırma Birliği
HTML	HyperText markup language	HyperText İşaretleme Dili
HTTP	HyperText transfer protocol	Hyper Text Transfer protokolü
IaaS	Infrastructure as a Service	Hizmet Olarak Alt Yapı
IAB	Internet Architecture Board	İnternet Mimarisi Kurulu
IANA	Internet Assigned Numbers Authority	İnternet Atanmış Numaralar Kurumu
IBP	Internet bandwidth provider	İnternet Bant Genişliği Sağlayıcısı
ICANN	Internet Corporation for Assigned Names and Numbers	İnternet Tahsisli Sayılar ve İsimler Kurumu
ICC	International Chamber of Commerce	Uluslararası Ticaret Odası
ICMEC	International Centre for Missing & Exploited Children	Uluslararası Kayıp ve İstismara Uğrayan Çocuklar Merkezi
ICT	information and communications technology	Bilgi ve İletişim Teknolojisi
IDC	International Data Corporation	Uluslararası Veri Şirketi
IDN	internationalised domain name	Uluslararasılaştırılmış Alan Adı
IEEE	Institute of Electrical and Electronic Engineers	Elektrik ve Elektronik Mühendisleri Enstitüsü
IETF	Internet Engineering Task Force	İnternet Mühendisliği Çalışma Grubu
IGC	Internet Governance Caucus	İnternet Yönetişimi Kurultayı
IGF	Internet Governance Forum	İnternet Yönetişimi Forumu
ILO	International Labour Organization	Uluslararası Çalışma Örgütü
IMF	International Monetary Fund	Uluslararası Para Fonu
IMPACT	International Multilateral Partnership against Cyber Threats	Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık
INHOPE	International Association of Internet Hotlines	Uluslararası İnternet Yardım Hatları Birliği
INSAFE	Network of Safer Internet Centres	Daha Güvenli İnternet Merkezleri Ağı
INTERPOL	International Criminal Police Organization	Uluslararası Suç Polisi Örgütü
NesNet	Internet of Things	Nesnelerin İnterneti
IP	Internet protocol	İnternet Protokolü
IPR	intellectual property rights	Fikri Mülkiyet Hakları

IPSec	Internet protocol security	İnternet Protokol Güvenliği
IPTV	Internet protocol television	İnternet Protokol Tabanlı Televizyon
IPv4	Internet protocol version 4	İnternet Protokolü sürüm 4
IPv6	Internet protocol version 6	İnternet Protokolü sürüm 6
IRP	independent review process	Bağımsız Değerlendirme Süreci
ISO	International Organization for Standardization	Uluslararası Standartlar Örgütü
ISP	Internet service provider	İnternet Servis Sağlayıcısı
ITAA	Information Technology Association of America	Amerika Bilgi Teknolojileri Derneği
ITRs	International Telecommunication Regulations	Uluslararası Telekomünikasyon Düzenlemeleri
ITU	International Telecommunication Union	Uluslararası Telekomünikasyon Birliği
ITU-D	ITU Telecommunication Development Sector	UTB Telekomünikasyon Geliştirme Sektörü
ITU-T	ITU Telecommunication Standardization Sector	UTB Telekomünikasyon Standartlaştırma Sektörü
IXP	Internet exchange point	İnternet Değişim Noktası
LACNIC	Latin American and Caribbean Network Information Centre	Latin Amerika ve Karayipler Ağ Bilgi Merkezi
LACTLD	Latin American and Caribbean ccTLDs Organization	Latin Amerika ve Karayipler ccTLD (Ülke Üst Düzey Alan Adı) Örgütü
LAN	local area network	Lokal Alan Ağı
LDCs	least developed countries	En Az Gelişmiş Ülkeler
LED	light emitting diode	Işık Yayan Diyot
LGBTQ	lesbian, gay, bisexual, trans, and queer	Lezbiyen, Gey, Biseksüel, Transseksüel ve Diğerleri
LIR	local Internet registry	Lokal İnternet Kütüğü
LPWAN	low-power wide-area network	Düşük Güç Tüketimli Alan Ağı
LTE	long-term evolution	Uzun Dönemli Evrilme
M3AAWG	Messaging, Malware, and Mobile Anti-Abuse Working Group	Mesajlaşma, Kötü Amaçlı Yazılım ve Mobil Anti-Kötüye Kullanım Çalışma Grubu
MDG	millennium development goal	Milyenyum Kalkınma Amacı
MIS-NET	Committee of Experts on Internet Intermediaries (CoE)	İnternet Araçları Uzmanları Komitesi (AK)
MLAT	Mutual Legal Assistance Treaty	Karşılıklı Yasal Yardım Paketi
MoU	memorandum of understanding	Mutabakat Anlaşması
NAT	network address translation	Ağ Adresi Çevirisi
NATO	North Atlantic Treaty Organization	Kuzey Atlantik Paketi
NIR	national Internet registry	Ulusal İnternet Kütüğü
NRI	Network Readiness Index (WEF)	Ağ Okunabilirlik Endeksi (WEF)
NSA	National Security Agency (USA)	Ulusal Güvenlik Ajansı (ABD)
NSF	National Science Foundation	ABD Ulusal Bilim Vakfı
NSI	Network Solutions Inc.	Ağ Çözümleri Şti
NTIA	National Telecommunications and Information Administration (USA)	ABD Ulusal Telekomünikasyon ve Enformasyon İdaresi
OAS	Organization of American States	Amerikan Devletleri Teşkilatı
OASIS	Organization for the Advancement of Structured Information Standards	Yapısal Bilgi Standartlarını Geliştirme Örgütü
ODR	online dispute resolution	Çevrimiçi Anlaşmazlık Çözümü
OECD	Organisation for Economic Co-operation and Development	Ekonomik İşbirliği ve Kalkınma Teşkilatı
OSCE	Organization for Security and Co-Operation in Europe	Avrupa Güvenlik ve İşbirliği Teşkilatı
OTT	over-the-top (services)	Zirvedeki Servis Sağlayıcılar

P2P	peer-to-peer	Denkten Denge
PaaS	Platform as a Service	Hizmet olarak Platform
PIPA	PROTECT IP Act	İP KORUMA Yasası
PKI	public key infrastructure	Kamu Temel Altyapısı
PLC	power line communications	Güç Hattı İletişimi
PPP	public private partnership	Kamu Özel Ortaklığı
PRISM	Personal Record Information System Methodology	Kişisel Bilgi Kayıt Sistemi Metodolojisi
PTI	Public Technical Identifiers (ICANN)	Kamu Teknik Tanımlayıcıları (ICANN)
QoS	Quality of Service	Hizmet Kalitesi
REMJA	Ministers of Justice or Other Ministers or Attorneys General of the Americas	Amerika Adalet Bakanları veya Diğer Bakanlar veya Başsavcıları
RFC	request for comments	Yorum İsteği
RFID	radio frequency identifiers	Radio Frekans Tanımlayıcıları
RIPE NCC	Réseaux IP Européens Network Coordination Centre	Avrupa İP Ağları Ağ Koordinasyon Merkezi
RIR	regional Internet registry	Bölgesel İnternet Kütüğü
RSC	Radio Spectrum Committee (EU)	Radio Spektrumu Komitesi (AB)
RSPG	Radio Spectrum Policy Group (EU)	Radio Spektrumu Politika Grubu (AB)
SaaS	Software as a Service	Hizmet olarak Yazılım
SCADA	Supervisory Control and Data Acquisition	Merkezi Denetim ve Veri Erişimi
SCO	Shanghai Cooperation Organisation	Şangay İşbirliği Örgütü
SDG	sustainable development goal	Sürdürülebilir Kalkınma Hedefleri
SGML	standard generalized markup language	Standart Genelleştirilmiş İşaretleme Dili
SMEs	small and medium-sized enterprises	Küçük ve Orta Büyüklükteki İşletme
SNA	system network architecture	Sistem Ağ Mimarisi
SOPA	Stop Online Piracy Act	ABD'de Çevrimiçi Korsanlığı Durdurma Yasası
SOXA	Sarbanes-Oxley Act	Sarbanes-Oxley Yasası
SSL	secure sockets layer	Güvenli Yuva (Soket) Katmanı
TACD	Trans Atlantic Consumer Dialogue	Trans Atlantik Tüketici Diyalogu
TASIM	Trans-Eurasian Information Super Highway	Trans Avrasya Süper Bilgi Yolu
TCP/IP	transmission control protocol/Internet protocol	İletim Kontrol Protokolü/İnternet Protokolü
TLD	top-level domain	Üst Düzey Alan Adı
TPP	Trans-Pacific Partnership	Trans Pasifik Ortaklığı
TRIPS	Trade-Related aspects of Intellectual Property Rights	Fikri Mülkiyet Haklarının Ticarete Konu Yönleri
TTIP	Transatlantic Trade and Investment Partnership	Trans Atlantik Ticaret ve Yatırım Ortaklığı
UDHR	Universal Declaration of Human Rights	Evrensel İnsan Hakları Beyannamesi
UDRP	Uniform Dispute Resolution Policy	Tekdüze uyumsuzluk Çözüm Politikası
UMAP	University Mobility in Asia and the Pacific	Asya ve Pasifik Üniversite Hareketliliği
US(A)	United States (of America)	(Amerika) Birleşik Devletleri
UN	United Nations	Birleşmiş Milletler
UNCITRAL	United Nations Commission on International Trade Law	Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu
UNCSTD	UN Commission on Science and Technology for Development	BM Kalkınma İçin Bilim ve Teknoloji Komisyonu
UNDP	United Nations Development Programme	Birleşmiş Milletler Kalkınma Programı
UNECSOC	UN Economic and Social Council	BM Ekonomik ve Sosyal Konseyi

UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific	Birleşmiş Milletler Asya ve Pasifik Ekonomik ve Sosyal Konseyi
UNGA	United Nations General Assembly	Birleşmiş Milletler Genel Kurulu
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Bilgi Teknolojileri ve Telekomünikasyon alanında Kalkınma Üzerine Hükümet Uzmanları Grubu
UNHRC	United Nations Human Rights Council	Birleşmiş Milletler İnsan Hakları Konseyi
UNODC	United Nations Office on Drugs and Crime	Birleşmiş Milletler Uyuşturucu ve Suçla Mücadele Ofisi
UNTOC	United Nations Convention against Transnational Organized Crime	Birleşmiş Milletler Uluslararası Suçla Mücadele konvensiyonu
UPC	universal product code	Evrensel Ürün Kodu
VAT	value added tax	Katma Değer Vergisi
VCR	videocassette recorder	Video Kaset Kaydedici
VoIP	Voice over Internet protocol	İP üzerinden ses iletimi
VPN	virtual private network	Sanal Özel Ağ
W3C	World Wide Web Consortium	Dünya Çapında Ağ Konsorsiyumu
WCIT	World Conference on International Telecommunications	Uluslararası Telekomünikasyon Konferansı
WEF	World Economic Forum	Dünya Ekonomik Forumu
WGIG	Working Group on Internet Governance	İnternet Yönetişimi Çalışma Grubu
WHO	World Health Organization	Dünya Sağlık Teşkilatı
WiMax	worldwide interoperability for microwave access	Mikrodalga Erişimi için Dünya Çapında Birlikte Çalışabilirlik
WIPO	World Intellectual Property Organization	Dünya Fikri Mülkiyet Hakları Örgütü
WLAN	wireless local area network	Kablosuz Lokal Ağ Bağlantısı
WML	wireless markup language	Kablosuz Biçimlendirme Dili
WSIS	World Summit on the Information Society	Dünya Bilgi Toplumu Zirvesi
WTO	World Trade Organization	Dünya Ticaret Örgütü
WTSA	World Telecommunication Standardization Assembly	Dünya Telekomünikasyon Standardlaştırma Konseyi
www	world wide web	Dünya Çapında Ağ
XHTML	eXtensible HTML	Genişletilebilir Hyper Tekt İşaretleme Dili
XML	eXtensible markup language	Genişletilebilir İşaretleme Dili
ZB	Zettabytes	Zeta Bayt

İnternet yönetiminde kullanılan kısa ad ve kısaltmaların daha kapsamlı bir listesi için bk. <https://www.diplomacy.edu/resources/books/internet-governance-acronym-glossary>



Yazar hakkında

Dr. Jovan Kurbalija DiploFoundation'nın kurucu direktörüdür ve Cenevre İnternet Platformu başkanıdır. Eski bir diplomat olan yazar, mesleki ve akademik geçmişli uluslararası hukuk, diplomasi ve bilgi teknolojisi alanlarındadır.

1992 yılında, Malta'daki Akdeniz Diplomatik Etütler Akademisi'nde Bilgi Teknolojisi ve Diplomasi Birimi'ni kurmuştur. On yıldan fazla eğitim, araştırma ve yayın yapmanın ardından, 2002'de Birim DiploFoundation'a dönüşmüştür.

1994 yılından beri, Dr. Kurbalija, BİT/İnternet'in diplomasi ve İnternet yönetişimi üzerindeki etkisi üzerine dersler vermektedir. Halen Belçika'nın Bruges şehrinde bulunan Avrupa Koleji'nde ve İsviçre'deki St Gallen Üniversitesinde ziyaretçi öğretim üyesi olarak bulunmaktadır. Malta'daki Akdeniz Diplomatik Çalışmalar Akademisi, Avusturya'daki Viyana Diplomatik Akademisi, Hollanda Uluslararası İlişkiler Enstitüsü (Clingendael), İsviçre Cenevre'deki Uluslararası ve Kalkınma Çalışmaları Enstitüsü, İtalya Torino BM Sistem Personeli Koleji ve Los Angeles'taki Güney Kaliforniya Üniversitesi'nde dersler vermiştir. 2005'ten bu yana DiploFoundation'ın İnternet Yönetişim Kapasitesi Geliştirme Programını kavramsallaştırmış ve yönetmiştir. Dr. Kurbalija'nın başlıca araştırma alanları arasında İnternet'e yönelik uluslararası bir rejimin geliştirilmesi, İnternet'in uluslararası diplomasi ve modern müzakerelerde kullanılması ve İnternet'in modern dünyaya etkisi yer almaktadır.

Dr. Kurbalija, aşağıdakileri içeren çok sayıda kitap, makale ve bölüm yayınlamış ve düzenlemiştir: Diplomatlar için İnternet Rehberi, Bilgi ve Diplomasi, BT'nin Diplomatik Uygulaması, Bilgi Teknolojisi ve Gelişmekte Olan Ülkelerin Diplomatik Hizmetleri, Modern Diplomasi ve Dil ve Diplomasi. Stefano Baldi ve Eduardo Gelbstein ile birlikte, İnternet ile ilgili çok çeşitli gelişmeleri kapsayan sekiz kitapçıdan oluşan Bilgi Toplumu Kütüphanesi'ni birlikte yazmıştır. jovank@diplomacy.edu

Çevirmen hakkında



ODTÜ Elektrik-Elektronik Mühendisliği Bölümü'nden şeref listesinde mezun olmuş, yine aynı bölümde Yüksek Lisans yapmıştır. Daha sonra ikinci Yüksek Lisansını İşletme alanında tamamlamış, İşletme alanındaki Doktora çalışmasından sonra akademik çalışmalarına devam ederek Yönetim Bilişim Sistemleri alanında 2013 yılında Doçent olmuştur. 1998 yılından bu yana profesyonel iş hayatında bulunan Dr.Özbilgin, çeşitli kamu kurumları ve özel kuruluşlarda bilişim ve teknoloji, dijital dönüşüm, ArGe ve inovasyon, iş geliştirme ve strateji alanlarında önemli görevler yapmıştır. Bu görevlerinin yanı sıra çeşitli üniversitelerde öğretim üyesi olarak dersler vermiş, önemli idari görevlerde ve akademik kurullarda yer almıştır. 2015 yılında HAVELSAN'a katılan Dr.Özbilgin, halen ArGe, Teknoloji ve Ürün Yönetimi Direktörü olarak görev yapmaktadır.

Dr.Özbilgin bu görevlerinin yanı sıra birçok önemli çalışma grupları ile sivil toplum kuruluşlarında sorumluluklar almıştır. Kamu Bilişim Derneği Başkanı olarak görev yapan Özbilgin, aynı zamanda ISACA'nın Türkiye Başkanlığını, Bilgi Güvenliği Derneği, Türkiye Bilişim Derneği, Finans Derneği gibi birçok STK'nın Yönetim Kurulu üyeliğini yürütmüştür. Dr. Özbilgin, Türkiye'de "Bilgi Teknolojileri Yönetişimi ve Denetimi", "Uluslararası Yönetim Bilişim Sistemleri Konferansı", "Kamu Bilişim Zirvesi" gibi birçok konferansın düzenlenmesinde görev almış, halen bu ve benzeri birçok etkinliği Düzenleme Komitesi'nde yer almaktadır.

Birçok ulusal ve uluslararası projeler yürüten Dr.Özbilgin, aynı zamanda ulusal ve uluslararası çeşitli kuruluşlara özellikle kamu ile ilgili projelerinde danışmanlık görevlerinde bulunmuştur. Kendisi özellikle yönetim bilişim sistemleri, dijital dönüşüm, teknoloji yönetimi ve inovasyon, iş geliştirme konularında çalışmakta olup, kendisinin birçok ulusal ve uluslararası konuşmaları ve yayınları bulunmaktadır.

İNTERNET YÖNETİŞİMİNE GİRİŞ

Jovan Kurbalija

İnternet Yönetişimine Giriş, bu alandaki ana konulara ve aktörlere kapsamlı bir genel bakış sunar. Rakamlar ve resimlerle desteklenmiş, açık ve erişilebilir bir şekilde yazılmış olan İnternet Yönetişiminin teknik, güvenlik, yasal, ekonomik, kalkınma, sosyo-kültürel ve insan hakları konularına odaklanır. Kısa bir giriş, ana soru ve tartışmaların bir özeti ve her konu için farklı görüş ve yaklaşımların bir incelemesini sunan kitap, İnternet Yönetişiminin analizi ve tartışılması için pratik bir çerçeve sunmaktadır.

1997'den bu yana, 3000'den fazla diplomat, bilgisayar uzmanı, sivil toplum aktivisti ve etkinlik bu kitapta sunulan metin ve yaklaşıma dayalı eğitim kurslarına katılmıştır. Kursların her bitimi ile birlikte, materyaller güncellenir ve geliştirilir, bu da kitabı İnternet Yönetişiminde tanıtım çalışmaları için bir öğretim kaynağı olarak özellikle faydalı kılar.

ISBN: 978-605-80156-0-9



9 786058 015609

DIPLO