YENİ SANAL SAVAŞ ALANI

Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?

Batı Balkanlar'da siber güvenlik (ve çevrimiçi radikalleşme) üzerine yapılan bir çalışmanın özeti

RegionalCooperationCouncil

İyi.
Daha İyi.
Bölgesel.

AB tarafından finanse edildi

Bu yayın AB tarafından finanse edildi. Sadece yazarlarının görüşlerini yansıtmaktadır. Burada yer alan bilgilerin herhangi bir şekilde kullanılmasından Bölgesel İşbirliği Konseyi ve AB sorumlu tutulamaz.

RegionalCooperationCouncil

Bu broşür, Batı Balkanlar'da şiddet içeren aşırılığı önleme ve aşırılıkla mücadeleyi amaçlayan IPA II 2016 Eylem Planı kapsamında Bölgesel İşbirliği Konseyi tarafından yaptırılan, **Batı Balkanlar'daki siber güvenliğe (ve çevrimiçi radikalleşmeye) ilişkin çalışmaya dayanarak hazırlandı.**

Bu broşürün temel amacı, Arnavutluk, Bosna-Hersek, Kosova*, Karadağ, Sırbistan ve Makedonya Eski Yugoslav Cumhuriyeti'ndeki (Batı Balkanlar 6 veya WB6) **siber güvenlik ve çevrimiçi radikalleşme durumu hakkında kapsamlı değerlendirme ve analiz sağlamak, ayrıca siber güvenliğin iyileştirilmesi ve çevrimiçi radikalleşmenin önlenmesi için önerilerde bulunmaktır.**

*Bu işaretleme statü hususunda tarafsız olup, Kosova'nın bağımsızlık ilanına ilişkin BMGK 1244 numaralı kararı ve Uluslararası Adalet Divanı'nın görüşleri ile uyumludur.

RegionalCooperationCouncil

İnternet Kullanımının Küresel Durumu

2015

2 Milyar
2015 yılında internet kullanıcı sayısı

2016

2,28 milyar
2016 yılında dünya çapında sosyal medya kullanıcı sayısı

2017

3,8 milyar
2017 yılında dünya çapında internet kullanıcı sayısı

%51
dünya nüfusunun %51'i

2022

6 milyar
2022 yılında beklenen internet kullanıcı sayısı

2030

7,6 milyar
2030 yılında internet kullanıcı sayısının beklenen artışı

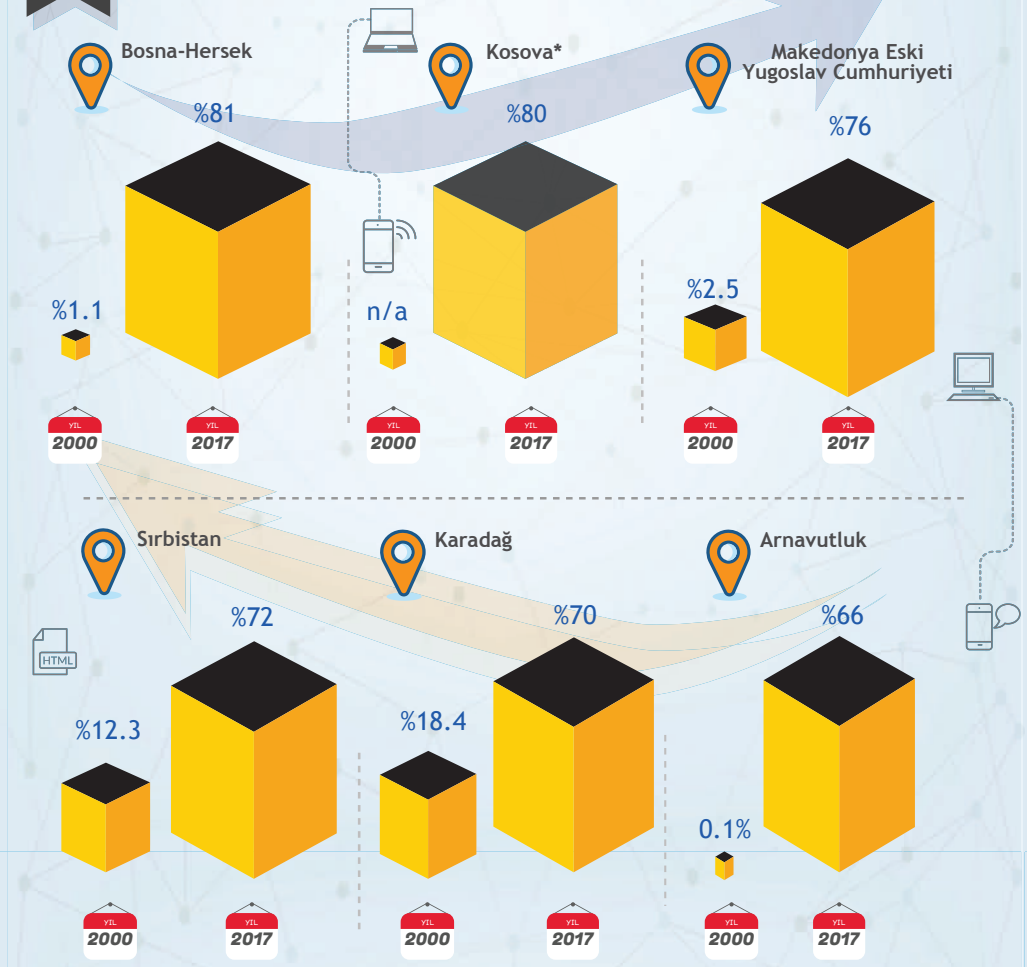
%90
Bu, dünyadaki **6 yaş** ve üzeri nüfusun yaklaşık % 90'ının İnternet kullanacağı anlamına geliyor

İnternet Kullanımının Bölgesel Durumu

ÖNEMLİ NOKTA!

2000 ile 2017 yılları arasında **Batı Balkanlar'daki İnternet kullanımında önemli bir artış olmuştur. İnternet kullanıcılarının sayısı**, ilgili ülkelerdeki **nüfusun %66 - %81'ine tekabül etmektedir**

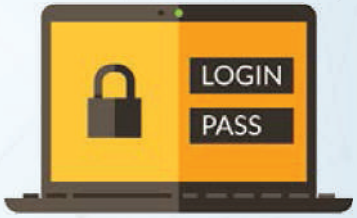
Bölgedeki İnternet kullanıcılarının yüzdesi:



Siber Güvenlik

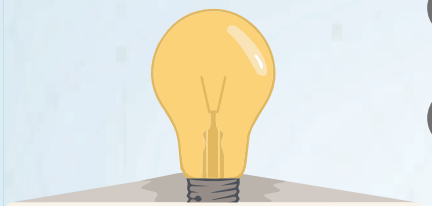
Siber saldırı ve siber suç gibi **sert veya kinetik saldırılara büyük ölçüde odaklanan**, oysa radikalleşme, nefret söylemi ve 'sahte haber' gibi çevrimiçi bilgi işlemlerini ihmal eden **siber güvenliğe ilişkin çağdaş kavramlar, amacına uygunluğu yitirmiştir**

"Yeni Sanal Savaş Alanı - Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?" isimli çalışma **siber güvenliğe ilişkin anlayışımızı iddialı bir şekilde genişletmektedir. Bu durum, İnternetin bilgi işlem operasyonlarındaki rolünün, siber güvenliğin diğer alanlarından ayrı olarak** görülmeyeceği ve görülmemesi gerektiğine dair RCC'nin gittikçe artan **farkındalığından kaynaklanmaktadır**



Peki, bölge böyle bir yaklaşıma ne kadar hazırdır?

Siber Güvenlik



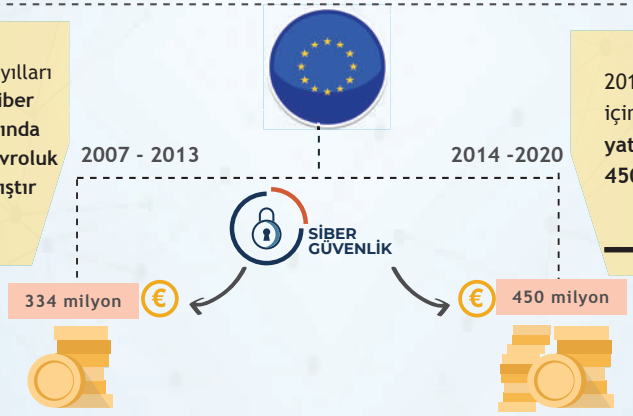
2015 İnternet kullanıcılarının **en yaygın endişeleri** üzerine yapılan 2015 Eurobarometer anketine göre;

%43 **Kişisel verilerin kötüye kullanılmasından** endişe duyanların oranı **% 43'tür**

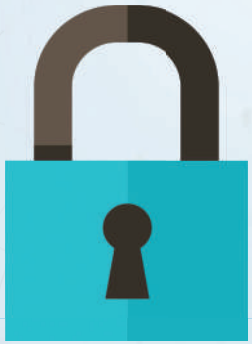
%42 **Çevrimiçi ödemelerin** güvenliği konusunda endişe duyanların oranı **% 42'dir**

%18 **İnternet bankacılığı** veya çevrimiçi ödeme konusunda endişe duymayanlar oranı **% 18'dir**

2007 ile 2013 yılları arasında **AB siber güvenlik alanında 334 milyon Avroluk yatırım yapmıştır**



2014-2020 dönemi için **planlanan ilave yatırımların tutarı 450 milyon avrodur**



CSIRT

Bilgisayar Güvenlik Olay Müdahale Ekipleri (CSIRTs)

WB6'daki Bilgisayar Güvenlik Olay Müdahale Ekipleri (CSIRT) görevleri bakımından birbirine çok benzer. Ancak işlevsellik düzeyleri bakımından farklılaşmaktadırlar.

WB6'daki ulusal CSIRT'lerden hiçbiri bağımsız yapıya sahip değildir ve hükümet içi konumları bölge çapında farklılıklar arz eder

YENİ SANAL SAVAŞ ALANI
Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?
RegionalCooperationCouncil

WB6
Üyelerine İlişkin Bilgi ve Bulguların Özeti

	ARNAVUTLUK	BOSNA - HERSEK	KOSOVA*	MAKEDONYA ESKİ YUGOSLAV CUMHURİYETİ	KARADAĞ	SIRBİSTAN
Siber Suçlara İlişkin Budapeşte Sözleşmesi	2002'de onaylandı, 7/24 irtibat makamı (POC) bulunuyor	2006'da onaylandı, 7/24 POC bulunuyor	7/24 POC bulunuyor	2004'te onaylandı, 7/24 POC bulunuyor	2010'da onaylandı, 7/24 POC bulunuyor	2009'da onaylandı, 7/24 POC bulunuyor
Ulusal CIRT	✓ 2016	Çok sınırlı işlevsellik, 2017	✓ 2016	✓ 2016	✓ 2012	✓ 2016
Siber Güvenlik Hukuku	✓ 2017'de kabul edildi.	✗	✓ 2010'da kabul edildi.	✗	✓ 2010'da kabul edildi	✓ 2016'da kabul edildi
Siber Güvenlik Stratejisi	Yasal düzenlemeler, 2015 - 2017	✗	Strateji ve eylem planı, 2016	Temmuz 2018'de kabul edilen strateji	2018-2021 Strateji ve eylem planı (ikinci strateji)	Var, ancak uygulama planı yok, 2017
Bilgi Güvenliği Konusunda Yüksek Eğitim	✗	✓	✓	✓	✓ disiplinler arası eğitim	✗
Aşırılığı Önleme / Terörizm Stratejisinde Siber/ Çevrimiçi suçlara Atıf	✓	✓	✓	✓	✓	✓
Temel Zorluklar	Teknik, finansal, uzmanlık sorunları ile hızlı personel döngüsü					

Siber Güvenlik Stratejisinin Uygulanmasına İlişkin Bölgedeki Zorluklar

- CSIRT'ler mali kaynak, yeterli kadro ve teknolojik kapasiteden yoksundur
- Olay raporlama: Şirketler özellikle olayın medyaya sızması nedeniyle yaşanabilecek itibar kaybından korkuyor; yasaların uygulanması hususunda güven eksikliği bulunuyor; saldırılar gerçekleştiğinde onları tespit etme kapasitesi eksik kalıyor
- Soruşturma ve prosedürler: beceri ve yetenek yeterliliği sorunu bulunuyor
- Kamu - özel ortaklıkları (PPP): Bölgedeki geleneksel PPP'ler yeterli değil; bu tür girişimlere yönelik talep eksik kalıyor; WB6 hükümetleri yerel bilgi ve iletişim teknolojileri uzmanlarına yeterince güvenmiyor (uluslararası uzmanlar tercih ediliyor)
- Eğitim: WB6'da bilgi ve iletişim teknolojileri ve buna bağlı güvenliğe odaklanan eğitim politikalarında belirgin bir eksiklik bulunuyor
- Medya: WB6'nın çoğunda siber güvenlik konusunda bilgiye dayalı raporlama eksikliği fark ediliyor
- Beyin göçü: Deneyimli bilgi ve iletişim teknolojileri uzmanlarının bölgeden göç oranları yüksektir
- Bölgede siber güvenlik riskleri hakkındaki farkındalık yetersizdir

YENİ SANAL SAVAŞ ALANI
Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?
RegionalCooperationCouncil

Çevrimiçi Radikalleşme

Şiddet yanlısı aşırıcılar ve teröristler...

bir süredir iletişim kurmak, işbirliği yapmak ve ikna etmek için **İnternetten faydalanmaktadır**. Nitekim Batı Balkanlar'da siber güvenlik (ve çevrimiçi radikalleşme) çalışması bu hususa odaklanmaktadır.

Radikalleşme süreçlerinde İnternetin rolü WB6 çapında belirgin olmakla birlikte, **kişisel etkileşimler önemini korumaktadır**

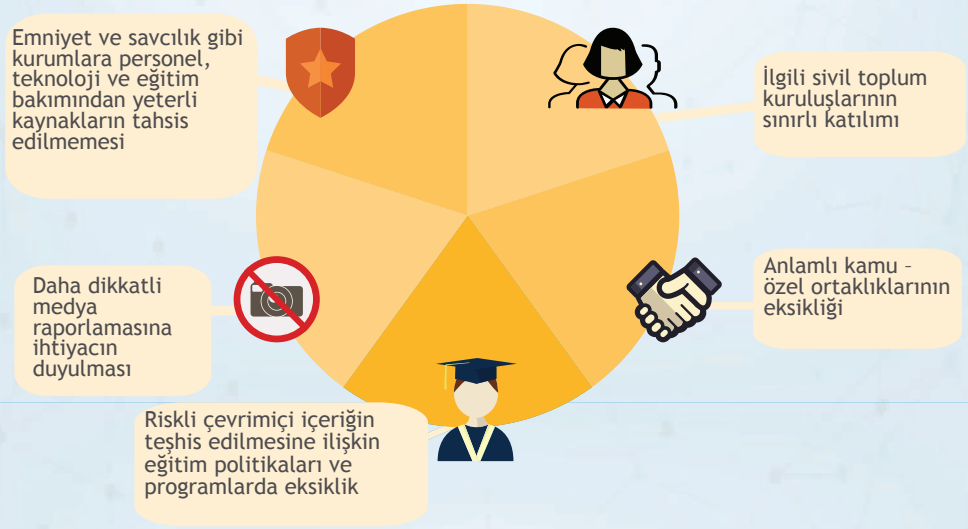
Radikalleşmeye ilişkin çağdaş tartışmalarda...

...'radikalleşme' çoğunlukla İslam adına yapılan terörizm ile bağlantılı kılınmakta, aşırı sağ gibi şiddet yanlısı aşırıcılık ve terörizm türlerinde ise radikalleşmenin çok daha az mevcut olduğu iddia etmektedirler

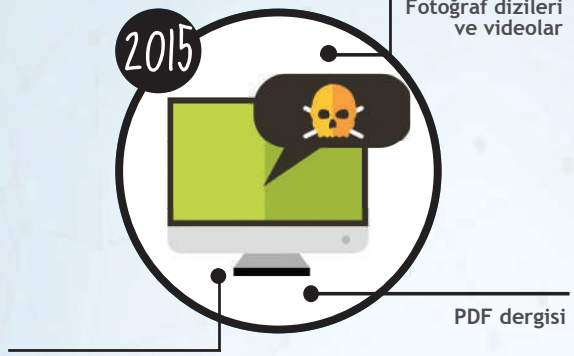
Tüm WB6 ekonomilerinde...

...ulusal düzeyde radikalleşme ve şiddet yanlısı aşırılığa karşı mücadele stratejileri bulunmakta, ancak **uygulama alanında geride kalmaktadırlar**

Radikalleşmenin önlenmesine ilişkin stratejilerin uygulanmasında karşılaşılan en önemli açıklar:

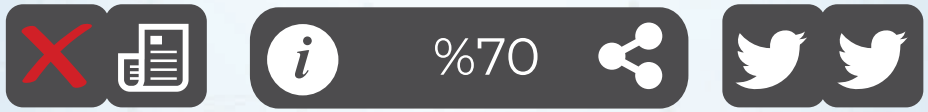


Çevrimiçi Radikalleşme

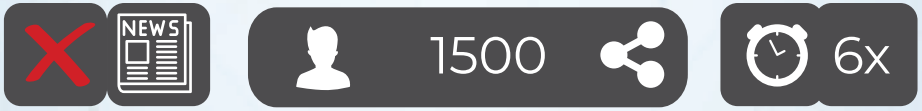


İslam devleti (DAEŞ), çevrimiçi varlığının zirve yaptığı 2015 yılında, fotoğraflar, infografik, PDF dergiler ve videolar dâhil olmak üzere, ayda yaklaşık 1200 içerik yayımlıyordu. Tabi, DAEŞ üyeleri çevrimiçi alanda tek başına aktif olan teröristler değildir.

Çeşitli şiddet yanlısı aşırıcılar, terörist gruplar ve onların destekçileri de mevcut olup, hâlihazırda çevrimiçi alanda değişik etkinliklere katılmış durumdalar



Yanlış bilgi, gerçek bilgiye kıyasla % 70 oranında tweet olarak yeniden paylaşılmaya müsaittir



Yanlış haber gerçek bir haberden ortalama olarak 6 kat daha hızlı yayılır ve 1500 kişiye ulaşır

2012 - 2017 döneminde Batı Balkanlar'dan yaklaşık 1000 kişi (erkek, kadın, çocuk, yaşlı) Suriye ve Irak'a seyahat etti. Bunların içinden 300'ü geri döndü, 200'den fazlası öldü, 400'e yakını oralarda kaldı, bazıları ise kayıplara karıştı

YENİ SANAL SAVAŞ ALANI
Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?
RegionalCooperationCouncil

ARNAVUTLUK

2017 YILINDA İNTERNET KULLANICI SAYISI

1,932,024

- Kendi başına bir siber güvenlik stratejisi bulunmuyor, ancak “Siber Güvenlik 2015 – 2017” isimli çalışma boşluğu dolduruyor
- Emniyette ve Genel Savcılıkta siber suçlara bakan özel birimler bulunmaktadır
- 10. ve 24. başlıklara ilişkin AB’nin 2018 değerlendirmesine göre, Arnavutluk bilgi güvenliği konusunda orta düzeyde hazırlıklıdır, ayrıca dijital gündem eylem planı ve e-devlet hizmetleriyle ilgili bazı ilerlemeler kaydetmiştir
- Siber suç olaylarının çoğunu sahtecilik, bilgisayar korsanlığı (hekleme), çevrimiçi taciz ve veri akışı ile ilgilidir

- Aşırıcılık yanlısı mesaj vakaların yaklaşık % 70’i doğrudan iletişim yoluyla, % 30’u da İnternet üzerinden yayılmıştır

- Arnavutluk’taki sosyal medya, aşırılık yanlısı içeriklerin yayılmasının en önemli kanalı değildir

WB6 üyelerine genel bakış

BOSNA-HERSEK

2017 YILINDA İNTERNET KULLANICI SAYISI

2,828,846

- Bölüm 10 ve 24 de AB 2018 değerlendirmesine göre Bosna-Hersek’in siber suçlar ve siber güvenlik tehditleri konularını ele alacak stratejik (devlet düzeyi) bir çerçeveden yoksun olduğu belirtilmektedir. Siber suçlar ile ilgili soruşturmaların çok nadir olduğuda söylenmektedir.
- Siber suçların türleri arasında DoS[1] ve DDos[2] saldırıları, İnternet sahtekarlığı, bilgisayar sistemine yetkisiz erişim, kredi kartı dolandırıcılığı, kablosuz ağ suiistimali, çocukları hedef alan çevrimiçi cinsel istismarlarla ilgili faaliyetler, çevrimiçi entelektüel mülkiyet hakları ihlalleri, sosyal ağ istismarı, kötü amaçlı yazılım dağılımı, kışkırtıcı nefret söylemi, uyuşmazlık veya hoşgörüsüzlük, ayrıca terörizm ve terör propagandasına yönelik kamu tahrikleri bulunmaktadır
- Bosna-Hersek’te bilgi güvenliği kültürü henüz gelişmiş değil. Olası etkileri hakkında farkındalık ve anlayış eksikliği belirgindir

- İnternetin Selefi ve Cihatçı ağlar dâhil, çeşitli çokuluslu ağların kurulmasını ve yayılmasını kolaylaştırdığına dair kanı yaygındır. Bosna-Hersek diasporasının önemli bir kısmı, Avusturya, Almanya, Hollanda, Slovenya ve İsveç’te bulunan Selefi gruplarıyla birlikte, İnternet üzerinden bağlanmış durumdadır
- Ancak topluluk bağları ve yüz yüze temaslar daha etkili olmuştur
- Bosna-Hersek’te belirgin bir şekilde artan milliyetçi retorik üzerinde de İnternet etkili olmuştur
- BIRN 2017’de, Batı Balkanlar’da kurulu bulunan ve etnik açıdan saf ulus devletleri, Neo-Nazizm’i, şiddetli homofobiyi ve diğer radikal sağ görüşlerin politikalarının propagandasını yapan 60’dan fazla İnternet sitesini tespit etmiştir

[1] Programlamada, hizmet engelleme saldırısı (DoS saldırı), failin İnternet’e bağlı bir ana bilgisayarın hizmetini geçici veya süresiz olarak engellemek suretiyle, bireysel kullanıcıların kendi bilgisayarlarına ve ağlarına erişimini kestiği siber saldırı durumudur.
[2] Dağıtık hizmet engelleme saldırısı (DDoS), İnternet trafiğini artırma veya ilgili altyapısına zarar vermek suretiyle, hedeflenen bir sunucunun, hizmetin veya ağın normal trafiğini bozmayı amaçlayan kötü niyetli bir saldırıdır.

MAKEDONYA ESKİ YUGOSLAV CUMHURİYETİ

2017 YILINDA İNTERNET KULLANICI SAYISI

1,583,315

SİBER GÜVENLİK

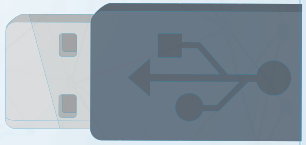
- 10. ve 24. başlıklara ilişkin AB'nin 2018 değerlendirmesinde, Makedonya Eski Yugoslav Cumhuriyeti'nin genel olarak AB standartlarıyla uyumlu olduğu, çevrimiçi çocuklara yönelik cinsel istismarı ve bilgisayar suçu gibi suçları cezalandırdığı belirtilmektedir. Ekonominin dijitalleşmesi de hızla ilerliyor
- Siber Güvenlik konusunda kapsamlı bir yasası yoktur. Ancak Temmuz 2018'de bir siber güvenlik stratejisi kabul edilmiştir
- Ulusal CSIRT 2016 yılında kurulmuştur
- Siber saldırılar çoğunlukla DoS ve kimlik hırsızlığı türlerinden oluşmaktadır. Ancak, kötü amaçlı yazılım dağıtımı artmaktadır ve birçok kullanıcı bu tehdidin farkında değildir

2017 YILINDA

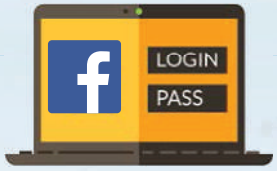
75

SİBER SALDIRI KAYEDİLMİŞTİR

ÇEVRİMİÇİ RADİKALLEŞME



- İnternet ve özellikle sosyal medya üzerinden aşırılık yanlısı ve terörist içeriğe kolay erişim vardır

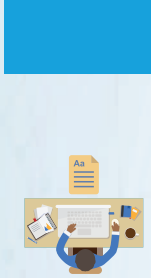


WB6 üyelerine genel bakış

KOSOVA*

2017 YILINDA İNTERNET KULLANICI SAYISI

1,523,373



- 10. ve 24. başlıklara ilişkin AB'nin 2018 değerlendirmesinde, Kosova'nın* siber güvenlik alanında çok olumlu ilerlemeler kaydettiği ve bu hususta çok iyi bir mevzuata sahip olduğu belirtiliyor. Ancak, henüz gerekli seviyeye erişememiş olan uygulama alanında sorunlar devam etmektedir

- Hükümet, emniyet siber suç birimi içinde 7/24 çalışan irtibat noktası atamış bulunmaktadır

- Kredi kartı sahtekârlığı, sahte haberler (örneğin medyaya sahte e-postalar üzerinden gönderilen haberler), bilgisayar ihlalleri, DDos saldırıları, kimlik hırsızlığı ve bunun gibi siber suçlar en yaygındır

- Özellikle İnternet servis sağlayıcıları açısından kamu ve özel sektör arasındaki ilişkiler iyidir. Ancak işbirliği olması gerektiği yerde henüz değildir

SİBER GÜVENLİK

ÇEVRİMİÇİ RADİKALLEŞME

- DAEŞ tarafından Arnavutça dilinde üretilen ve ağırlıklı olarak Kosova odaklı olan çevrimiçi içerikler, Arnavutluk, Kosova* ve Makedonya Eski Yugoslav Cumhuriyeti'nde Arnavutça konuşanları hedeflemektedir

- Sosyal medyanın önemli rolüne ek olarak, DAEŞ'in Kosova'daki* faaliyetlerine ilişkin değişik raporlarda, radikalleşme ve personel alımı süreçlerinde geleneksel kitle iletişim araçlarının önemine de değinilmektedir

- Kosova* yabancı savaşçıların radikalleşme süreçlerinde İnternet önemli bir rol oynamıştır

KARADAĞ

2017 YILINDA İNTERNET KULLANICI SAYISI

439,624

Yıllara ve saldırı türlerine göre istatistikler

	WEB SİTELERİ VE DAEŞ'E SALDIRILAR	ÇEVRİMİÇİ DOLANDIRICILIK	SOSYAL HESAPLARIN KÖTÜYE KULLANILMASI	UYGUNSUZ ÇEVRİMİÇİ İÇERİKLER	KÖTÜ AMAÇLI YAZILIM	DİĞER
2013	5	3	10	-	1	3
2014	5	6	20	5	-	6
2015	6	17	37	19	17	36
2016	18	20	36	14	50	25
2017 (1 Eylüle kadar)	90	13	25	4	245	8
Toplam	124	59	128	42	313	78

2017 YILINDA

385

SİBER SALDIRI KAYDEDİLMİŞTİR

- 10. ve 24. başlıklara ilişkin AB'nin 2018 değerlendirmesinde, Karadağ siber güvenliği konusunda esaslı bir değerlendirmeye yer verilmemiştir
- 2017'de hükümet Bilgi Güvenlik Konseyi'ni oluşturmuştur
- Karadağ'daki özel sektör siber güvenlik alanında çok ilerleme kaydetmiştir. Bazı IT servis sağlayıcıları bu alanda en az 15 yıldır öncülük etmektedir
- Karadağ mevzuat ve politikalar bakımından siber güvenlik alanında hızla ilerlemektedir

#3 Karadağ'da üç ana aşırıcılık türü bulunmaktadır:

- Şiddet yanlısı tekfircilik (bu raporda 'şiddet yanlısı cihatçılık' olarak isimlendirilmiştir)
- Şiddet yanlısı olmayan Salafizm
- Panslavizm ve Ortodoks aşırıcılığı

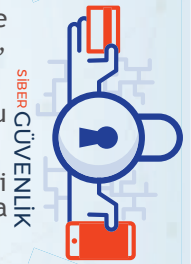
Son aşırıcılık türü bağlamında, bazı Karadağlılar doğu Ukrayna'daki yabancı savaşçı birliklerine katılmışlardır

SIRBİSTAN

2017 YILINDA İNTERNET KULLANICI SAYISI

6,325,816

- 10. ve 24. başlıklara ilişkin AB'nin 2018 değerlendirmesinde, Sırbistan'ın siber suçlar konusunda henüz bir strateji kabul etmediği belirtilmektedir
- Personel sorunları nedeniyle CSIRT sınırlı işlevselliğe sahiptir
- Ulusal CSIRT, Elektronik Haberleşme ve Posta Hizmetlerine İlişkin Cumhuriyet Ajansı'nın bünyesinde kurulmuştur, ancak diğer CSIRT'ler de Sırbistan'da mevcuttur
- Siber suçlarla mücadele için Özel Savcılık Bürosu bulunmaktadır
- Hükümetin bilgi güvenliği alanındaki farkındalığı göreceli olarak yeni olmakla birlikte, bu husus güvenlik alanında yeni bir meydan okuma olarak kabul edilmiştir
- Özel sektör ile hükümet arasında iyi bir işbirliği vardır ve gelişim göstermeye devam etmektedir

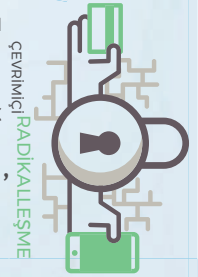


2017 YILINDA

20

SİBER SALDIRI KAYDEDİLMİŞTİR

- Sancak bölgesindeki gençler arasında yapılan bir kamuoyu araştırmasının sonuçları, ankete katılanların yarısından fazlasının (% 52,6), aşırı görüş ve içeriğinin yayılmasında çevrimiçi platformları önemli gördüğünü göstermiştir
- Aynı ankete katılanların neredeyse yarısı (% 46,7) çevrimiçi alanda sosyal medya platformlarının radikal propaganda için en önemli araç olduğunu düşünmektedir
- Ankete katılanların oldukça daha küçük bir kısmı 'dini müesseselerin' aşırıcı mesajları yayabildiğine (% 7,1) veya bu türden mesajların 'topluluk' içinde yaygın oluğuna (% 8,3) inanıyor.
- 2017 yılında BIRN, Sırpça dilde yayın yapan 30'un üzerinde aşırı sağ web sitesi tespit etmiştir



10

YEARS

Powered
by RCC.int

BÖLGESEL İŞBİRLİĞİ KONSEYİ

Trg Bosne i Hercegovine 1/V

71000 Saraybosna, Bosna-Hersek

+387 33 561 700 +387 33 561 701 rcc@rcc.int

rcc.int RegionalCooperationCouncil @rccint RCCSec Regional Cooperation Council

RegionalCooperationCouncil

Siber Güvenliğin Geliştirilmesi İçin Öneriler

ULUSAL DÜZEYDE

- Planlama aşamasında uygun maliyetli stratejiler ve eylem planları geliştirilmeli ve bu planlar ilgili fonlarla güçlendirilmelidir
- Siber olayları raporlama yapıları oluşturulmalı ve/veya iyileştirilmelidir
- Farkındalık artırılmalıdır
- İlgili taraflar arasında ağlar oluşturarak, mevcut uzmanlıklar güçlendirilmelidir.
- Kamu – özel işbirliği imkanları tespit edilip geliştirilmeli ve sinerji oluşturulmalıdır
- Bilgi ve iletişim teknolojisi ile siber güvenliğe ilişkin eğitim yaklaşımı gözden geçirilmelidir

BÖLGESEL DÜZEYDE

- Mevcut yapılar çerçevesinde, bölgesel işbirliğine daha stratejik bir yaklaşım geliştirilmelidir
- Uluslararası toplumun bölgesel stratejiye uygun desteği sağlanmalıdır
- Bölgesel düzeyde bir mükemmellik merkezi kurulmalıdır

Çevrimiçi Radikalizmin Önlenmesi İçin Öneriler

ULUSAL DÜZEYDE

- Radikalleşmeyle mücadele ve terörizme katılımı engelleme konularında AB stratejisine daha fazla uyum sağlamak için, şiddet içeren aşırılığı önleme stratejileri gözden geçirilmelidir
- Siber Güvenlik Stratejileri ile tutarlılığı ve tamamlayıcılığı sağlamak amacıyla, terörizmle mücadele ve şiddet içeren aşırılığı önleme stratejileri gözden geçirilmelidir
- Terörizmle mücadele stratejileri ve mevzuatı, bilgi sistemleri üzerine saldırıları da kapsayacak şekilde gözden geçirilmelidir
- Tüm bunların iyileştirilmesi maksadıyla, özel şirketler, sivil toplum kuruluşları ve medya ile var olan ilişkiler gözden geçirilmeli ve ortaklaşa uygun eylemler geliştirilmelidir
- Grupların veya bireylerin desteğini almak için, toplumsal sorunlar gözden geçirilerek, onlara çözümler üretilmelidir
- Siber güvenlik eğitimi içine eleştirel düşünme dahil edilmelidir

BÖLGESEL DÜZEYDE

- Aşırıcılık ve aşırıcılık yanlısı çevrimiçi içeriklere karşı tutarlı bir yaklaşım sergilenmelidir
- Terörist içeriğe erişimi mümkün olduğunca zor ve masraflı kılmak için, istihbarat ve ispata dayalı yaklaşım benimsenmelidir
- Büyük teknoloji şirketleri ve terörizme karşı mücadele forumları ile daha iyi ilişkiler geliştirilmelidir
- Batı Balkanlar Yönlendirme/Tavsiye Birimi kurulmalıdır
- Batı Balkanlar Güvenlik Gündemi geliştirilip kabul edilmelidir
- Radikalleşme Farkındalık Ağı'nın bir benzeri Batı Balkanlar için geliştirilmelidir

YENİ SANAL SAVAŞ ALANI
Batı Balkanlar'da Siber Güvenlik Alanında Çevrimiçi Radikalleşme Nasıl Önlenebilir?
RegionalCooperationCouncil