NOVO VIRTUELNO bojno polje

Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?

Sažeti pregled studije o kibernetičkoj sigurnosti (i radikalizaciji na internetu) na Zapadnom Balkanu

RegionalCooperationCouncil

Good.
Better.
Regional.

finansira EU

Ovu publikaciju finansira Evropska unija i u njoj su izražena samo mišljenja autora. Vijeće za regionalnu saradnju i Evropska unija ne mogu se smatrati odgovornim za upotrebu informacija sadržanih u ovom dokumentu.

RegionalCooperationCouncil

Brošura je **zasnovana** na studiji o kibernetičkoj sigurnosti (i radikalizaciji na internetu) na Zapadnom Balkanu, koju je naručilo Vijeće za regionalnu saradnju, kao dio Regionalnog djelovanja na sprječavanju i borbi protiv nasilnog ekstremizma na Zapadnom Balkanu u sklopu instrumenta IPA II za 2016. godinu.

Glavni **cilj** studije na kojoj se temelji ova brošura je da se pruži **sveobuhvatan presjek** i **analiza** situacije u pogledu **kibernetičke sigurnosti** i **radikalizacije na internetu** u Albaniji, Bosni i Hercegovini, Kosovu*, Crnoj Gori, Srbiji i Bivšoj Jugoslovenskoj Republici Makedoniji (**šest ekonomija Zapadnog Balkana** ili ZB6) te da se **daju preporuke** za **unaprijeđenje kibernetičke sigurnosti** i **spriječavanje radikalizacije na internetu**.

* Ovaj naziv ne prejudicira stavove o statusu i u skladu je sa Rezolucijom Vijeća sigurnosti Ujedinjenih nacija 1244 i mišljenjem Međunarodnog suda pravde o kosovskoj deklaraciji o nezavisnosti.

RegionalCooperationCouncil

Osvrt na globalno internetsko okruženje

2015

2 Milijarde
broj internet korisnika u 2015.

2.28 Milijarde
korisnika društvenih medija u cijelom svijetu 2016. godine.

2016

3.8 Milijarde
broj internet korisnika u svijetu u 2017. što je

51%
svjetske populacije

2017

2022

6 Milijarde
očekivani broj internet korisnika do 2022.

7.6 Milijarde
očekivani broj internet korisnika do 2030.

2030

90%
stanovništva u svijetu će u.dobi 6 i više godina koristiti internet.

Osvrt na regionalno internetsko okruženje

VAŽNA NAPOMENA!

Značajno **povećanje korištenja interneta** na **Zapadnom Balkanu** zabilježeno između 2000. i 2017. godine, sa brojem **korisnika interneta** između **66% i 81% stanovništva**

% *.korisnika interneta u regionu*

Bosna i Hercegovina
81%
1.1%
GODINA 2000
GODINA 2017

Kosovo *
80%
n/a
GODINA 2000
GODINA 2017

Bivša Jugoslovenska Republika Makedonija
76%
2.5%
GODINA 2000
GODINA 2017

Srbija
72%
12.3%
GODINA 2000
GODINA 2017

Crna Gora
70%
18.4%
GODINA 2000
GODINA 2017

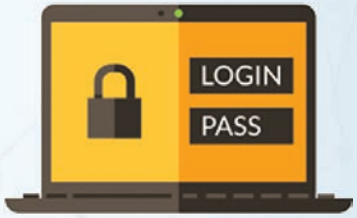
Albanija
66%
0.1%
GODINA 2000
GODINA 2017

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

Kibernetička sigurnost

Savremeni **koncepti kibernetičke sigurnosti**, koji su u velikoj mjeri usmjereni na **napade na infrastrukturu i kinetičke napade**, kao što su kibernetički napadi i kibernetički kriminal, a u kojima su izostavljeni **internetski napadi zasnovani na informacijama**, kao što je radikalizacija na internetu, govor mržnje i lažne vijesti, više ne odogovaraju svrsi.

Novo virtuelno bojno polje – Kako spriječiti radikalizaciju u sklopu kibernetičke sigurnosti Zapadnog Balkana ambiciozno **proširuje poimanje kibernetičke sigurnosti** koje sada **obuhvata oboje**, što proizilazi iz **svjesnosti Vijeća za regionalnu saradnju** da se **uloga interneta** u internetskim napadima zasnovanim na informacijama ne može i **ne treba** shvatati **odvojeno** od **drugih oblasti kibernetičke sigurnosti**.



U kojoj je mjeri region spreman za ovakav pristup?

Kibernetička sigurnost

2015 Anketa Eurobarometera iz 2015. godine o **najčešćim brigama** korisnika:

43% zabrinuto zbog **zloupotrebe ličnih podataka**

42% zabrinuto za sigurnosti **plaćanja putem interneta**

18% nema **nikakvih** briga o **internetskom bankarstvu** ili plaćanju putem interneta

Između 2007. i 2013. **EU je uložila 334 miliona eura** u **kibernetičku sigurnost**

Planirana dodatna ulaganja u periodu između 2014. i 2020. iznose **450 miliona eura**

CSIRT

TIMOVI ZA ODGOVOR NA RAČUNARSKE SIGURNOSNE INCIDENTE (CSIRTs)

Funkcije svih **timova za odgovor na računarske sigurnosne incidente** (CSIRT) u **šest ekonomija Zapadnog Balkana** su veoma **slične;** međutim, stepen njihove **funkcionalnosti nije jednak** u svim ekonomijama.

Niti jedan nacionalni **CSIRT** u šest ekonomija Zapadnog Balkana nije **samostalna agencija** i imaju različit položaj u sklopu organa vlasti u regionu

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

Kibernetička sigurnost

Pregled

relevantnih informacija i nalaza za svaku od šest ekonomija Zapadnog Balkana

	ALBANIJA	BOSNA I HERCEGOVINA	KOSOVO*	BIVŠA JUGOSLOVENSKA REPUBLIKA MAKEDONIJA	CRNA GORA	SRBIJA
Konvencija o kibernetičkom kriminalu iz Budimpešte	Ratificirana 2002. Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici	Ratificirana 2006. Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici	Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici	Ratificirana 2004. Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici	Ratificirana 2010. Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici	Ratificirana 2009. Mjesto za kontakt, raspoloživo 24 sata na dan, sedam dana u sedmici
Nacionalni tim za odgovor na računarske incidente (CIRT)	✓ 2016.	Veoma ograničena funkcionalnost 2017.	✓ 2016.	✓ 2016.	✓ 2012.	✓ 2016.
Zakon o kibernetičkoj sigurnosti	✓ Usvojen 2017.	✗	✓ usvojen 2010.	✗	✓ usvojen 2010.	✓ usvojen 2016.
Strategija o kibenetičkoj sigurnosti	Postoje dokumenti politike, 2015-2017.	✗	Strategija i akcioni plan 2016.	Strategija usvojena u julu 2018.	Strategija i akcioni plan 2018-2021. (druga strategija)	Da, nema akcionog plana 2017.
Tercijarno obrazovanje o informacionoj sigurnosti	✗	✓	✓	✓	✓ multidisciplinarno	✗
Strategija za borbu protiv nasilnog ekstremizma i terorizma sadrži reference o kibernetičkom prostoru odnosno internetu	✓	✓	✓	✓	✓	✓
Glavni izazovi	Tehnički, finansijski, stručni kao i dostupnost i zadržavanje kadrova					

Regionalni izazovi u provedbi strategije kibernetičke sigurnosti

- Timovima za odgovor na računarske sigurnosne incidente (CSIRT) nedostaje sredstava, dovoljno osoblja i tehnološkog kapaciteta
- Izvještavanje o incidentima: firme se boje štete po svoj ugled u slučaju da incidenti izađu u javnost, nedostatak povjerenja u provedbu zakona, nedostatak kapaciteta da se napadi prepoznaju kada se dese
- Istrage i postupci: nema dovoljno vještina i sposobnosti
- Javno-privatno partnerstvo (JPP): nedostatak tradicije JPP u regionu, nepostojanje potražnje za ovakvim inicijativama, vlasti ne prepoznaju stručnjake iz oblasti informacionih i komunikacionih iz šest ekonomija Zapadnog Balkana (prednost se daje stranim stručnjacima)
- Obrazovanje: očigledan nedostatak obrazovne politike usmjerene na informacione i komunikacione tehnologije i prateću sigurnost u šest ekonomija Zapadnog Balkana
- Mediji: primjećeni nedostatak informisanog izvještavanja o kibernetičkoj sigurnosti u većini ekonomija ZB6
- Odliv mozgova: visoke stope migracije iskusnih stručnjaka iz oblasti informacionih i komunikacionih tehnologija iz regiona
- Nedostatak svijesti o rizicima za kibernetičku sigurnost u regionu

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

Radikalizacija na internetu

Nasilni ekstremisti i teroristi...

...već neko vrijeme **koriste internet** za komunikaciju, saradnju i pridobijanje pristalica, a to je upravo i tema kojom se bavi *studija o kibernetičkoj sigurnosti (i radikalizaciji na internetu) na Zapadnom Balkanu*.

Uloga interneta u procesima **radikalizacije očigledna** je **u svih šest ekonomija Zapadnog Balkana**, međutim, **lični kontakt je i dalje važan**.

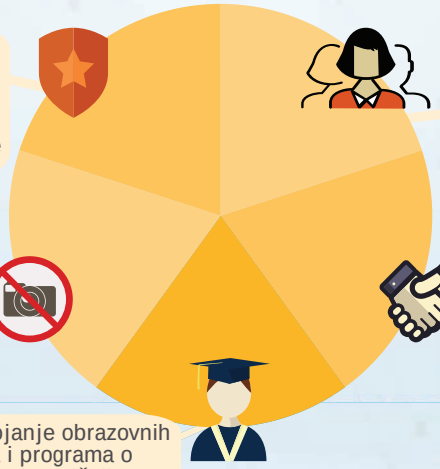
Kritičari današnjeg diskursa o radikalizaciji...

...tvrde da se '**radikalizacija**' uglavnom povezuje sa **nasilnim** terorizmom **džihadista** dok je mnogo manje prisutna u raspravama o **drugim oblicima nasilnog ekstremizma** i terorizma, kao što je **ekstremna desnica**.

Sve osim dvije ekonomije Zapadnog Balkana...

...imaju nacionalne strategije za **borbu protiv radikalizacije i/ili nasilnog ekstremizma** - ali **zaostaju** u njihovoj **provedbi**.

Najznačajniji nedostaci vezani za provedbu strategija za borbu protiv radikalizacije:



ograničena sredstva tijela kao što su policija i tužioci u pogledu kadrovske popunjenosti, tehnologije i edukacije

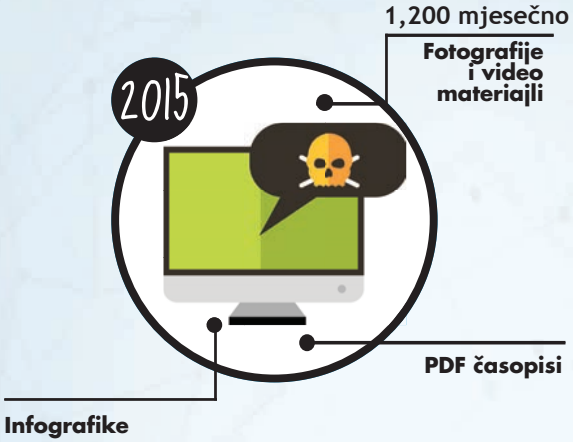
ograničeno odgovarajuće učešće civilnog društva

potreba za pažljivijim medijskim izvještavanjem

nedostatak značajnih javno-privatnih partnerstava

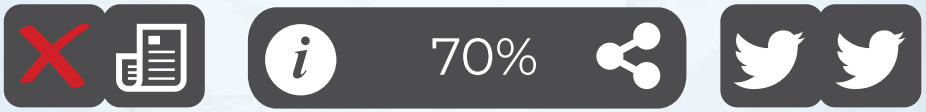
nepostojanje obrazovnih politika i programa o utvrđivanju rizičnih sadržaja na internetu

Radikalizacija na internetu

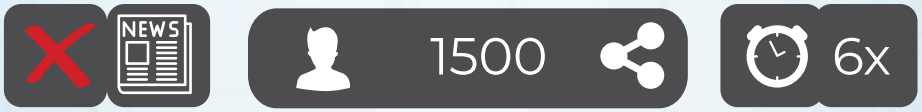


Na vrhuncu svoje snage na internetu 2015. godine, Islamska država je mjesečno proizvodila oko 1.200 primjeraka sadržaja, uključujući nizove fotografija, infografike, časopise u PDF formatu i video zapise.

Islamska država nije, naravno, jedini terorista aktivan na internetu. Postoje brojni različiti nasilni ekstremisti i terorističke grupe i njihove pristalice koji trenutno učestvuju u različitim aktivnostima na internetu.



70% je veća vjerovatnoća da se proslijedi lažna u odnosu na istinitu informaciju.



Lažna priča u prosjeku dopre do 1.500 osoba šest puta brže od istinite priče.

U periodu između 2012. i 2017. godine oko **1.000** pojedinaca (muškaraca, žena, djece, starijih) sa Zapadnog Balkana otputovalo je u Siriju i Irak, od kojih se oko **300** vratilo, više od **200** je ubijeno, oko **400** je ostalo, dok se za neke smatra da su nestali.

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

ALBANIJA

INTERNET KORISNICI U DECEMBRU 2017.

1,932,024

KIBERNETIČKA SIGURNOST

- Nema strategiju kibernetičke sigurnosti kao takvu, ali u njenom nedostatku dovoljan je dokument o kibernetičkoj sigurnosti za period 2015-2017. godina
- Posebne jedinice za kibernetički kriminal postoje u policiji i Tužilaštvu
- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da je Albanija umjereno spremna za informacionu sigurnost te da je određeni napredak ostvaren u vezi sa akcionim planom za digitalnu agendu i uslugama e-vlade
- Većina slučajeva kibernetičkog kriminala odnosi se na prevaru, hakovanje, uhođenje na internetu i ometanje podataka

RADIKALIZACIJA na internetu

- Do širenja ekstremističkih poruka je u 70% slučajeva došlo kroz direktnu komunikaciju i u oko 30% slučajeva posredstvom interneta

- Društveni mediji nisu najvažniji kanal za širenje ekstremističkog sadržaja u Albaniji

Pregled za svaku ekonomiju ZB6 - *Kibernetička sigurnost* i *Radikalizacija na internetu*

BOSNA I HERCEGOVINA

INTERNET KORISNICI U DECEMBRU 2017.

2,828,846

- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da Bosni i Hercegovini nedostaje strateški okvir [na državnom nivou] da bi se pozabavila pitanjem kibernetičkog kriminala i prijetnjama kibernetičkoj sigurnosti. Istrage kibernetičkog krinimala su navodno veoma rijetke
- Glavni oblici kibernetičkog kriminala obuhvataju DoS[1] i DDos[2] napade, prevaru na internetu, neovlašten pristup računarskim sistemima, prevare sa kreditnim karticama, zloupotrebu bežične mreže, aktivnosti vezane za seksualno zlostavljanje djece na internetu, kršenje prava intelektualnog vlasništva na internetu, zloupotrebu društvenih mreža, distribuciju štetnih softvera, poticanje na mržnju, neslaganje ili netoleranciju, javno poticanje na terorizam i terorističku propagandu
- U Bosni i Hercegovini još uvijek nema kulture informacione sigurnosti – nepostojanje svijesti i razumijevanja o potencijalnim uticajima

KIBERNETIČKA SIGURNOST

RADIKALIZACIJA na internetu

- Opšteprihvaćeno je da je internet olakšao uspostavljanje i širenje velikog broja različitih transnacionalnih mreža, uključujući mreže selefista i džihadista. Velika bosanskohercegovačka dijaspora, sa značajnim kontigentima selefista u Austriji, Njemačkoj, Nizozemskoj, Sloveniji i Švedskoj, povezana je putem interneta.
- Međutim, veze u zajednici i kontakti uživo su važniji
- Uloga interneta u povećanoj nacionalističkoj retorici očiglednoj u BiH je također sugerisana
- BIRN je 2017. godine locirao više od 60 internet stranica na Zapadnom Balkanu na kojima se promovira ideja etnički čistih nacionalnih država, neonacizma, nasilne homofobije i drugih radikalnih desničarskih politika

[1] U računarstvu, uskraćivanje servisa (DoS) je kibernetički napad gdje izvršilac nastoji da mašinu ili mrežni resurs uskrati najmenjenim korisnicima na način što se privremeno ili neograničeno ometaju usluge onoga ko je povezan na internet.
[2] Distribuirani napad uskraćivanja servisa (DDoS) je zlonamjeran pokušaj da se omete normalan saobraćaj ciljanog servera, servisa ili mreže tako što se oni ili infrastruktura oko njih preopterete internetskim saobraćajem.

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

BIVŠA JUGOSLOVENSKA REPUBLIKA MAKEDONIJA

INTERNET KORISNICI U DECEMBRU 2017.

1,583,315

KIBERNETIČKA SIGURNOST

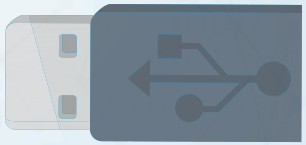
- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da je krivični zakon Bivše Jugoslovenske Republike Makedonije generalno u skladu sa standardima EU, i u njemu se, između ostalog, seksualno zlostavljanje djece na internetu i računarski kriminal određuju kao krivična djela. Digitalizacija ove ekonomije brzo napreduje.
- Nema krovnog zakona o kibernetičkoj sigurnosti, ali je u julu 2018. godine usvojena strategija kibernetičke sigurnosti
- Tim za odgovor na računarske sigurnosne incidente (CSIRT) formiran 2016. godine
- DoS napadi i krađe identiteta činili su većinu kibernetičkih napada, uz povećnu distribuciju štetnih softvera iako kod većine korisnika ne postoji svijest o ovoj prijetnji

zabilježeno

75

kibernetičkih napada u 2017.

RADIKALIZACIJA na internetu



- Jednostavan pristup ekstremističkom i terorističkom sadržaju putem interneta, a naročito društvenih medija

Pregled za svaku ekonomiju ZB6 - *Kibernetička sigurnost* i *Radikalizacija na internetu*

KOSOVO *

INTERNET KORISNICI U DECEMBRU 2017.

1,523,373

- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da je Kosovo* ostvarilo veoma pozitivan napredak u oblasti kibernetičke sigurnosti te da ima veoma dobre zakonske propise. Najvažnije pitanje se, međutim, odnosi na njihovo provođenje, koje još uvijek nije na potrebnom nivou.

- Vlasti su u sklopu policijske jedinice za kibernetički kriminal imenovale mjesto za kontakt koje je dostupno 24 sata na dan, sedam dana u sedmici

- Najčešći oblik kibernetičkog kriminala čine prevare sa kreditnim karticama, lažne vijesti (npr. putem krivotvorenih elektronskih poruka medijima), upad u računare, DDoS napadi, krađe identiteta, itd.

- Odnosi između javnog i privatnog sektora su dobri, naročito u pogledu pružalaca internetskih usluga. Međutim, saradnja još uvijek nije na nivou na kome bi trebala biti.

KIBERNETIČKA SIGURNOST

RADIKALIZACIJA na internetu

- Sadržaj na internetu na albanskom jeziku kojeg je pripremila Islamska država bio je usmjeren na osobe koje govore albanski jezik u Albaniji, na Kosovu* i u Bivšoj Jugoslovenskoj Republici Makedoniji, sa posebnim naglaskom u kontekstu Kosova*

- Osim značajne uloge medija, u brojnim izvještajima o aktivnostima Islamske države na Kosovu* pominje se važnost tradicionalnih masovnih medija u procesima radikalizacije i regrutacije

- Internet je odigrao značajnu ulogu u procesu radikalizacije stranih boraca sa Kosova*

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

MONTENEGRO

INTERNET KORISNICI U DECEMBRU 2017.

439,624

Statistički podaci po godinama i vrsti napada

	NAPADI NA INTERNET STRANICE i IS	PREVARA PUTEM INTERNETA	ZLOUPOTREBA PROFILA NA DRUŠTVENIM MREŽAMA	NEPRIKLADAN SADRŽAJ NA INTERNETU	ŠTETNI SOFTVER (*MALVER*)	OSTALO
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 (do 01. sept.)	90	13	25	4	245	8
TOTAL	124	59	128	42	313	78

zabilježeno **385** kibernetičkih napada u 2017. godini

- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da Crna Gora nije obuhvatila značajniju procjenu u vezi sa kibernetičkim prostorom i kibernetičkom sigurnosti
- 2017. godine vlada je formirala Savjet za informacionu bezbjednost
- Privatni sektor u Crnoj Gori je veoma napredan u oblasti kibernetičke sigurnosti, sa nekim od pružalaca usluga informacionih i komunikacionih tehnologija koji u ovom području djeluju najmanje 15 godina
- Crna Gora brzo napreduje u oblasti kibernetičke sigurnosti sa zakonodavnog stanovišta, ali i sa stanovišta politika

KIBERNETIČKA SIGURNOST

RADIKALIZACIJA na internetu

#3 U Crnoj Gori postoje tri glavna oblika ekstremizma:

- nasilni tekfirizam (u izvještaju se koristi pojam 'nasilni džihadizam')
- nenasilini selefizam
- i panslavizam i pravoslavni ekstremizam

Što se tiče trećeg oblika, neki Crnogorci su se priključili kontigentu stranih boraca u istočnoj Ukrajini.

Pregled za svaku ekonomiju ZB6 - *Kibernetička sigurnost* i *Radikalizacija na internetu*

SRBIJA

INTERNET KORISNICI U DECEMBRU 2017.

6,325,816

- U procjeni EU za 2018. godinu za poglavlja 10 i 24 navodi se da Srbija tek treba da usvoji strategiju o kibernetičkom kriminalu
- Tim za odgovor na računarske sigurnosne incidente (CSIRT) je ograničene funkcionalnosti zbog problema sa kadrovskom popunjenošću
- Nacionalni Tim za odgovor na računarske sigurnosne incidente (CSIRT) smješten je u Republičkoj agenciji za elektronske komunikacije i poštanske usluge, ali je u Srbiji prisutan i veliki broj drugih CSIRT-ova
- Postoji Posebno tužilaštvo za borbu protiv kibernetičkog kriminala
- Oblast informacione sigurnosti smatra se relativno novim područjem podizanja svijesti za Vladu, i to područjem koje se vidi kao novi sigurnosni izazov
- Uglavnom postoji dobra saradnja između privatnog sektora i vlade, i poboljšava se

KIBERNETIČKA SIGURNOST

zabilježeno **20** kibernetičkih napada u 2017

SPAM

- Nalazi ispitivanja javnog mnijenja provedenog među mladima sa Sandžaka pokazali su da je više od polovine ispitanika (52,6%) smatralo internetske platforme ključnima za širenje ekstremističkih stavova i sadržaja
- Skoro polovina ispitanika (46,7%) istog ispitivanja smatrala je da su za širenje ekstremističke propagande na internetu najvažniji alati bile platforme društvenih medija
- Znatno manji broj ispitanika smatrao je da su „vjerski objekti" značajni za širenje ekstremističkih poruka (7,1%) ili da su takve poruke široko raspostranjene „u zajednici" (8,3%)
- 2017. godine BIRN je locirao 30 i više ekstremno desničarskih internet stranica na srpskom jeziku

RADIKALIZACIJA na internetu

NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

Preporuke za poboljšanje kibernetičke sigurnosti

Nacionalni nivo

- Izraditi troškovno učinkovite strategije i akcione planove tokom faze planiranja i takve planove poduprijeti odgovarajućim sredstvima
- Uspostaviti i/ili poboljšati strukture za izvještavanje o kibernetičkim incidentima
- Podizati svijesti
- Iskoristiti postojeću stručnost kroz stvaranje mreža zainteresovanih strana
- Utvrditi i razviti javno-privatna partnerstva (JPP) i uspostaviti sinergije
- Revidirati obrazovni pristup informacionim i komunikacionim tehnologijama i kibernetičkoj sigurnosti

Regionalni nivo

- Razviti strateški pristup regionalnoj saradnji u sklopu postojećih okvira
- Dobiti podršku međunarodne zajednice strategiji regiona
- Uspostaviti regionalni centar izvrsnosti

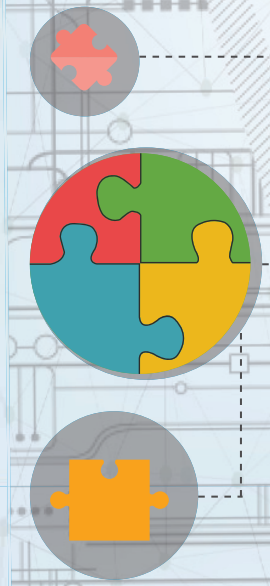
Preporuke za sprječavanje radikalizacije na internetu

Nacionalni nivo

- Revidirati strategije borbe protiv nasilnog ekstremizma kako bi se osigurala veća usklađenost sa strategijom EU za borbu protiv radikalizacije i regrutovanja terorista
- Revidirati strategije za borbu protiv terorizma i nasilnog ekstremizma kako bi se osigurala usklađenost i komplementarnost sa strategijama kibernetičke sigurnosti
- Revidirati strategije i zakonske propise u oblasti borbe protiv terorizma kako bi se osiguralo da su njima obuhvaćeni i napadi na informacione sisteme
- Revidirati postojeće odnose sa firmama iz privatnog sektora, organizacijama civilnog društva i medijima kako bi se pripremile konkretne aktivnosti da se ti odnosi unaprijede
- Revidirati i pripremiti odgovore kojima bi se riješili društveni problemi koje grupe ili pojedinci mogu iskoristiti za zadobijanje podrške
- Uvrstiti kritičko razmišljanje u obrazovanje o kibernetičkoj sigurnosti

Regionalni nivo

- Osigurati usklađen pristup ekstremizmu i ekstremističkom sadržaju na internetu
- Zauzeti pristup zasnovan na podacima i dokazima kako bi se pristup terorističkom sadržaju učinio što težim i skupljim
- Uspostaviti bolji odnos sa vodećim visokotehnološkim firmama i forumima za borbu protiv terorizma
- Uspostaviti jedinicu Zapadnog Balkana za postupanje u slučajevima prijavljenog internetskog sadržaja
- Pripremiti i usvojiti program sigurnosti Zapadnog Balkana
- Uspostaviti Mrežu za podizanje svijesti o radikalizaciji za Zapadni Balkan



NOVO VIRTUELNO BOJNO POLJE
Kako spriječiti radikalizaciju na internetu u sklopu kibernetičke sigurnosti Zapadnog Balkana?
RegionalCooperationCouncil

10

YEARS

Powered
by RCC.int

Vijeće za regionalnu saradnju

Trg Bosne i Hercegovine 1/V

71000 Sarajevo, Bosna i Hercegovina

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

rcc.int RegionalCooperationCouncil @rccint RCCSec Regional Cooperation Council

RegionalCooperationCouncil