НОВО ВИРТУЕЛНО бојно поле

Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?

Резиме на Студијата за информатичка безбедност (и онлајн радикализација) во земјите на Западен Балкан

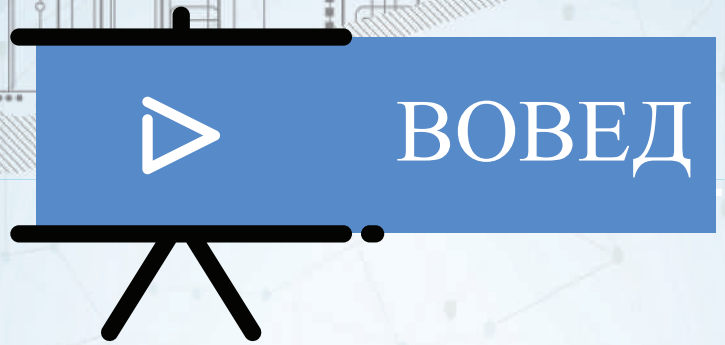
RegionalCooperationCouncil

Добро.
Подобро.
Регионално.

проект финансиран од ЕУ

Оваа публикација е финансирана од ЕУ. Таа ги одразува само ставовите на авторот(ите). Советот за регионална соработка и ЕУ не сносат одговорност за каква било примена на содржаните информации.

RegionalCooperationCouncil



ВОВЕД

Оваа брошура се заснова на Студијата за информатичката безбедност (и онлајн радикализацијата) во земјите на Западен Балкан, нарачана од Советот за регионална соработка, во рамките на регионалната акција на ИПА II 2016 регионална активност за превенција и борба против насилен екстремизам (P/CVE) во земјите на Западен Балкан.

Главната **цел** на Студијата, која е основа и на оваа брошура, е да обезбеди **сеопфатен преглед** и **анализа** на ситуацијата во врска со **информатичката безбедност** и **онлајн радикализацијата** во Албанија, Босна и Херцеговина, Косово*, Црна Гора, Србија и Поранешната Југословенска Република Македонија (**Западен Балкан 6 -ЗБ6** или WB6) и да **обезбеди препораки** за **подобрување на информатичката безбедност** и **спречување на онлајн радикализацијата.**

* Оваа ознака не претставува заземање став во врска со статусот и е во согласност со Резолуцијата 1244 на Советот за безбедност на ОН и мислењето на МСП за косовската декларација за независност.

RegionalCooperationCouncil

Преглед на глобалното онлајн опкружување

2015 — **2 милијарди** интернет-корисници во 2015 год.

2016 — **2,28 милијарди** корисници на социјални медиуми во 2016 година, на светско ниво

2017 — **3,8 милијарди** интернет-корисници на светско ниво во 2017 год. или **51%** од светската популација

2022 — **6 милијарди** очекуван број на интернет-корисници до 2022 год.

2030 — **7,6 милијарди** очекуван пораст на бројот на интернет-корисници до 2030 год.

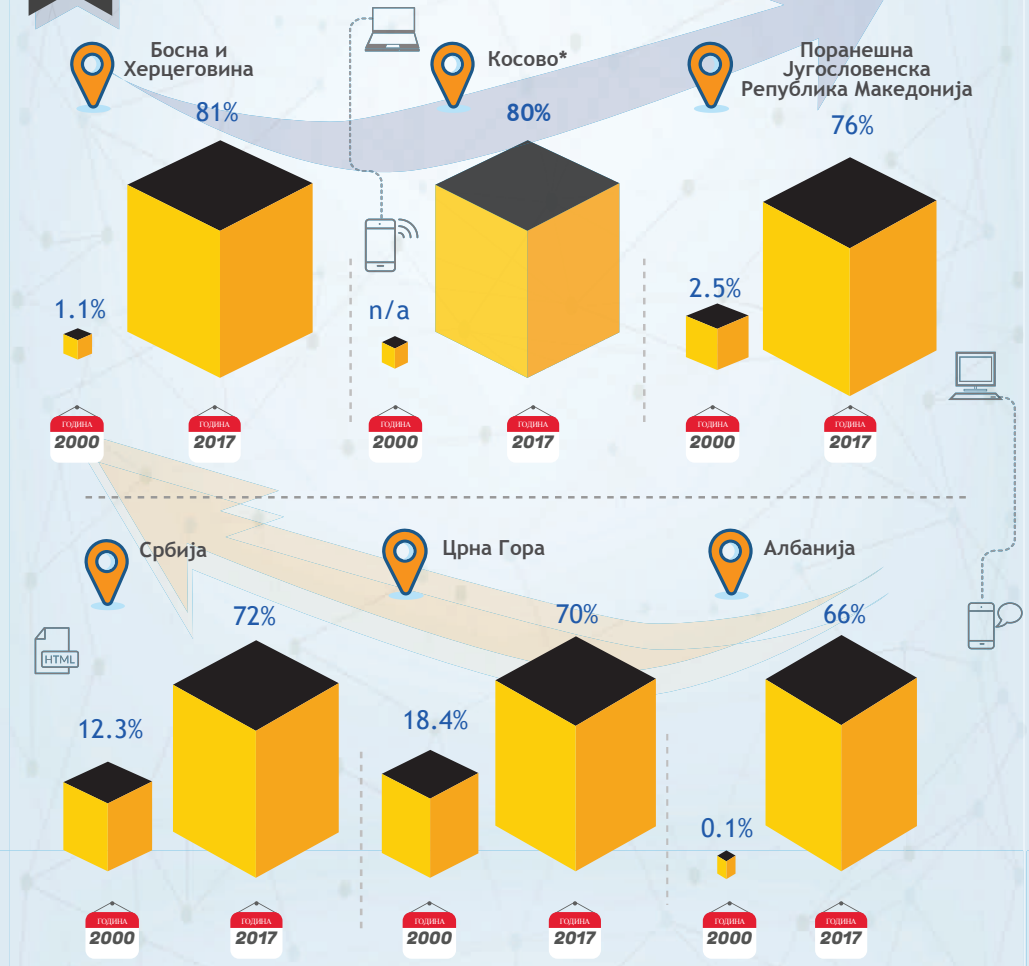
90% од светското население на возраст над 6 години ќе користи интернет

Преглед на регионалното онлајн опкружување

Важно!

Во периодот меѓу 2000 и 2017 год., во земјите на Западен Балкан е забележан значителен **пораст** на бројот на **интернет- корисниците**, кој се движи од **66% до 81%** од населението.

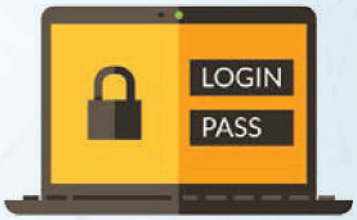
% *на интернет-корисници во регионот:*



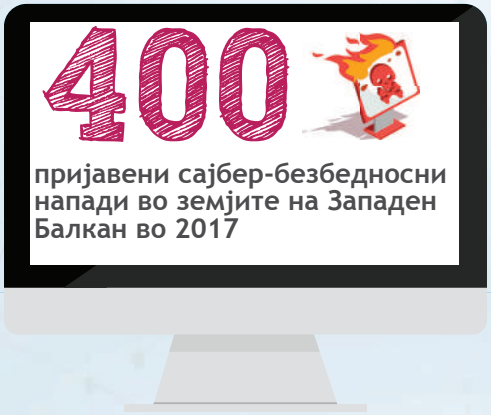
Информатичка безбедност

Современите **концепции** на информатичката **безбедност,** кои во голема мера се фокусираат на **напади на хард-дискови или кинетички напади**, како што се сајбер напади и компјутерски криминал а ги пропуштаат **информациите за онлајн операции**, како што се онлајн радикализација, говор на омраза и лажни вести, повеќе не се целисходни.

Во ***Ново виртуелно бојно поле - Како да се спречи онлајн радикализацијата во областа на*** информатичката ***безбедност во земјите на Западен Балкан*** амбициозно **се проширува** нашето **разбирање на информатичката безбедност** и се **опфаќаат обете** области, што произлегува од подигнувањето на **свеста во рамките на СРС** дека **улогата на интернетот** во информатичките операции не може и **не треба** да се разгледува **изолирано** од **други области** на **информатичката безбедност.**



Дали регионот е подготвен за овој пристап?



Информатичка безбедност

2015 Истражување на Евробарометар за 2015 година, **најчестите проблеми на корисниците на** интернет:

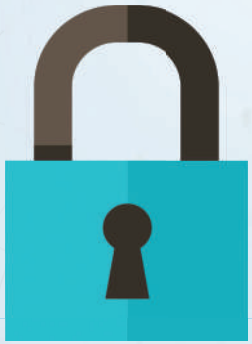
43% о проблеми во врска со злоупотреба на нивните лични податоци

42% проблеми со безбедноста на нивните онлајн плаќања

18% Немаат проблем со онлајн банкарството или онлајн плаќање

Помеѓу 2007 и 2013 година, **ЕУ инвестираше 334 милиони €** во **информатичка безбедност**

Планирани понатамошни инвестиции во периодот 2014 до 2020 година, во висина од **450 милиони €**



CSIRT

ТИМОВИ ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ (CSIRTs)

Функциите на сите **Тимови за одговор на компјутерски инциденти** (CSIRTs) во земјите на Западен Балкан 6 се многу слични; сепак, нивните нивоа на функционалност **не се конзистентни** во економиите на сите овие 6 држави.

Ниеден од националните тимови CSIRTs во ЗБ6 не е **самостојна агенција,** но нивното позиционирање во владите е различно во целиот регион.

НОВО ВИРТУЕЛНО БОЈНО ПОЛЕ
Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?
RegionalCooperationCouncil

Информатичка безбедност

Синопсис
на релевантни информации и наоди за секоја од ЗБ6

	АЛБАНИЈА	БОСНА И ХЕРЦЕГОВИНА	КОСОВО*	ПОРАНЕШНА ЈУГОСЛОВЕНСКА РЕПУБЛИКА МАКЕДОНИЈА	ЦРНА ГОРА	СРБИЈА
Конвенцијата за компјутерски криминал од Будимпешта	Ратификувана 2002 24/7 контакт центар	Ратификувана 2006 24/7 контакт центар	24/7 контакт центар	Ратификувана 2004 24/7 контакт центар	Ратификувана 2010 24/7 контакт центар	Ратификувана 2009 24/7 контакт центар
Тим за одговор на компјутерски инциденти - CSIRT, на државно ниво	✓ 2016	Многу ограничена функционалност 2017.	✓ 2016	✓ 2016	✓ 2012	✓ 2016
Закон за информатичка безбедност	✓ Усвоена 2017	✗	✓ Усвоена 2010 година	✗	✓ Усвоена 2010 година	✓ Усвоена 2016 година
Стратегија за информатичка безбедност	Постојат стратегиско-политички акти, 2015-2017	✗	Стратегија и акционен план 2016	Стратегија усвоена во јули 2018 година	Стратегија и акционен план 2018-2021 (2ра страт.	Да, нема акционен план 2017
Зто ниво на образование за информатичка безбедност	✗	✓	✓	✓	✓ мултидисциплинарно	✗
CVE / Во стратегијата за борба против тероризмот е вклучена референца за сајбер/онлајн	✓	✓	✓	✓	✓	✓
Клучни предизвици	Технички, финансиски, експертиза и пристап и задржување на персоналот					

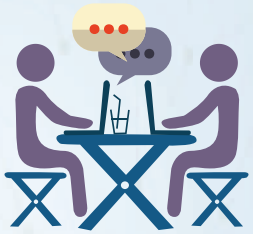
Регионални предизвици при спроведувањето на стратегијата за информатичка безбедност

- Тимовите за одговор на компјутерски инциденти - CSIRTs немаат доволно средства, доволно персонал, ниту технолошки капацитет
- Инцидентно известување: компаниите особено стравуваат од репутациска штета во случај на протекување на информации во медиуми; немање доверба во спроведувањето на законот, немање капацитет за идентификување на нападите кога ќе се случат
- Истраги и процедури: најголем проблем – недостатокот на вештини и способности
- Јавно-приватни партнерства (ЈПП): немање традиција на ЈПП во регионот; нема побарувачка за такви иницијативи; владите не ги признаваат ИКТ експертите во економиите на земјите на Западен Балкан 6 (даваат предност на меѓународни експерти)
- Образование: очигледен недостаток на образовни политики, кои се фокусираат на ИКТ и со неа поврзаната безбедност во земјите на Западен Балкан 6
- Медиуми: забележан е недостаток на известување за информатичка безбедност од страна на познавачи, во поголемиот дел од земјите на Западен Балкан
- Одлив на мозоци: високи стапки на миграција на искусни ИКТ професионалци од регионот
- Недостаток на свест за ризиците во врска со информатичката безбедноста во регионот

НОВО ВИРТУЕЛНО БОЈНО ПОЛЕ
Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?
RegionalCooperationCouncil

Онлајн радикализација

Насилни екстремисти и терористи...



...веќе извесно време го **користат интернетот** за да комуницираат, да соработуваат и убедуваат. Токму тоа *е во фокусот на Студијата за информатичката безбедност (и онлајн радикализацијата) во земјите на Западен Балкан.*

Очигледна е **улогата на интернетот** во **процесите на** радикализација **ширум земјите на Западен Балкан 6**, но **личната комуникација останува многу важна.**

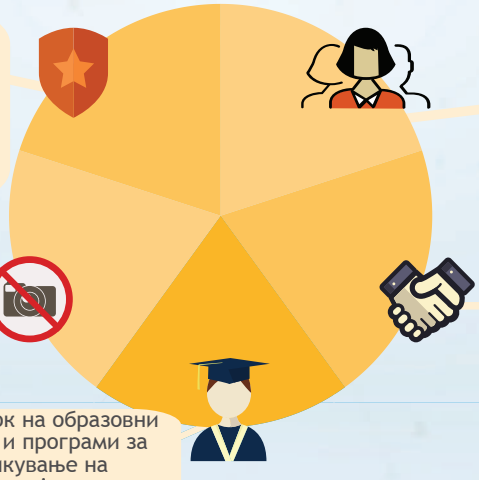
Критичарите на современиот радикален...

...дискурс тврдат дека **„радикализацијата“** најчесто се поврзува со **насилен џихадистички** тероризам и е многу помалку распространет во дискусиите **во врска со други видови** на **насилен екстремизам** и тероризам, како што е **екстремната десница.**

Со исклучок на две од земјите на Западен Балкан 6...

...сите имаат државни стратегии за спречување на радикализација и / или насилен екстремизам - но **заостануваат** со нивното **спроведување.**

Најзначајни недостатоци поврзани со спроведувањето на стратегии за борба против радикализацијата:



ограничени ресурси за органите, како што се полицијата и обвинителите, во однос на кадровско екипирање, технологија и обука

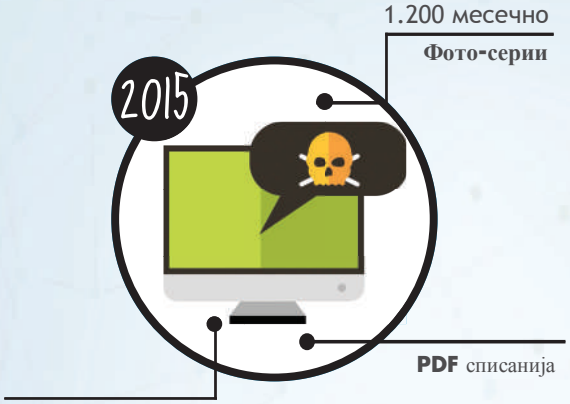
ограничено соодветно учество на граѓанското општество

потреба за повнимателно информирање од страна на медиумите

недостаток на значајни јавно-приватни партнерства

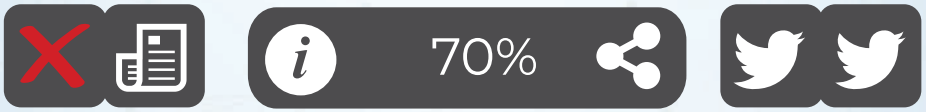
недостаток на образовни политики и програми за идентификување на ризични онлајн содржини

Онлајн радикализација

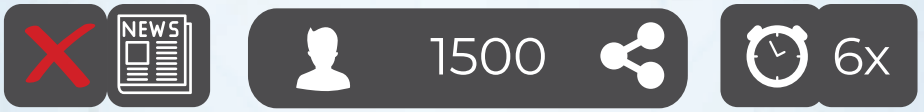


На врвот на нивната онлајн моќ во 2015 год., Исламската држава (ИСИС) продуцираше приближно 1.200 официјални изданија месечно со различни содржини, меѓу кои фото-серии, инфографики, PDF списанија и видеа. Се разбира, ИСИС не се единствените терористи кои се активни онлајн.

Постојат најразлични насилни екстремистички и терористички групи и нивните поддржувачи во моментов се ангажирани во голем бр. разнородни онлајн активности.



Лажните вести имаат 70% поголема веројатност да бидат преземени и пренесени од вистинските.



Во просек, лажните приказни допираат до бројка од 1.500 луѓе, 6 пати побрзо од вистинските

Во периодот 2012-2017 год. **околу 1.000** поединци (мажи, жени, деца, постари лица) од Западен Балкан отпатувале за Сирија и Ирак, од кои околу **300** се вратиле, повеќе од **200** се убиени, приближно **400** се останати, додека некои се сметаат за исчезнати.

НОВО ВИРТУЕЛНО БОЈНО ПОЛЕ
Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?
RegionalCooperationCouncil

АЛБАНИЈА

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

1,932,024

- Нема посебен документ, стратегија за информатичка безбедност, но во недостаток на стратегија, документот Стратегија за информатичка безбедност 2015-2017 ја пополнува празнината
- Во државната полиција и во Јавното обвинителство функционираат посветени единици за компјутерски криминал
- Во Оценката на ЕУ за 2018 год., во врска со поглавјата 10 и 24, се вели дека Албанија е умерено подготвена за информатичка безбедност, а постигнат е извесен напредок во врска со акцискиот план за дигитална агенда и услугите на е-влада
- Најголемиот број случаи на компјутерски криминал се измама, хакирање, онлајн демнење и интерференција во податоците

- Ширењето на екстремистички пораки се одвива по пат на директна комуникација во околу 70% од случаите и околу 30% преку интернет
- Социјалните медиуми **не се** најважен канал за ширење на екстремистички содржини во Албанија

Поединечен преглед за секоја од земјите на Западен Балкан 6

БОСНА И ХЕРЦЕГОВИНА

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

2,828,846

- Во Оценката на ЕУ 2018 год., во врска со поглавјата 10 и 24, се вели дека Босна и Херцеговина нема стратешка [на државно ниво] рамка за решавање на прашањето за компјутерски криминал и информатичко-безбедносни закани. Истрагите во областа на компјутерскиот криминал, наводно, остануваат многу ретки.
- Главните видови на компјутерски криминал вклучуваат DoS[1] и DDos[2] напади, интернет-измама, неовластен пристап до компјутерски системи, измами со кредитни картички, злоупотреба на безжични мрежи, онлајн активности поврзани со сексуална злоупотреба на деца, онлајн прекршување на права на интелектуална сопственост, злоупотреба на социјална мрежа, дистрибуција на малициозен софтвер (malware), поттикнување на омраза, раздор или нетолеранција и јавно поттикнување на тероризам и терористичка пропаганда
- Во БиХ сè уште нема култура на информатичка безбедност - недостаток на свест и разбирање на потенцијалните влијанија

- Се препознава дека интернетот е средството што го олесни воспоставувањето и ширењето на бројни транснационални мрежи, меѓу кои и салафистички и џихадистички мрежи. Големата дијаспора на БиХ, со значајни салафистички контингенти во Австрија, Германија, Холандија, Словенија и Шведска, го користи интернет за меѓусебно поврзување
- Сепак, односите во заедницата и личните контакти имаат посилно влијание
- Нагласена е улогата на интернетот и во зајакнувањето на националистичката реторика во БиХ
- Во 2017 година, BIRN ги лоцираше седиштата на повеќе од 60 веб-страници кои промовираа идеи за етнички чисти национални држави, неонацизам, насилна хомофобија и други радикални политички десничарски политики, во земјите од Западен Балкан.

[1] Во информатиката, нападот наречен одбивање на услуга (denial of service, DoS) е информатички напад во кој сторителот се обидува да постигне машината или мрежниот ресурс да станат недостапни за своите наменети корисници, со привремено или бесконечно нарушување на услугите на домаќинот (host) поврзан на интернет.
[1] Широко распространето откажување на услугата (distributed denial of service- DDoS) е злонамерен обид за нарушување на нормалниот сообраќај на целниот сервер, услуга или мрежа, со преоптоварување на целта или нејзиното инфраструктурно опкружување со голем прилив на интернет-сообраќај.

ПОРАНЕШНА ЈУГОСЛОВЕНСКА РЕПУБЛИКА МАКЕДОНИЈА

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

1,583,315

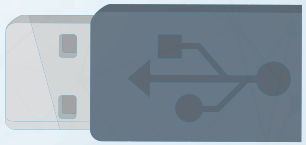
ИНФОРМАТИЧКА БЕЗБЕДНОСТ

- Во Оценката на ЕУ за 2018, во врска со поглавјата 10 и 24, се вели дека Кривичниот законик на Поранешната Југословенска Република Македонија е во голема мерка усогласен со стандардите на ЕУ, криминализирајќи ја онлајн сексуалната злоупотреба на деца и компјутерскиот криминал, меѓу другите злосторства. Дигитализацијата на економијата напредува брзо
- Нема сеопфатен закон за информатичка безбедност, но стратегијата за овој вид безбедност е усвоена во јули 2018 година
- Во 2016 година е основан Тимот за одговор на компјутерски инциденти - CSIRT
- Поголемиот дел од информатичките напади се од типот DoS и fishing, но дистрибуцијата на злонамерен софтвер (malware) се зголемува поради недостаток на свест за оваа закана кај многу корисници

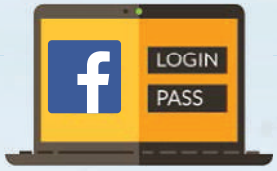
75

сајбер-напади регистрирани во 2017 година

ОНЛАЈН РАДИКАЛИЗАЦИЈА



- Лесен пристап до екстремистички и терористички содржини преку интернет, особено преку социјалните медиуми



Поединечен преглед за секоја од земјите на Западен Балкан 6

КОСОВО*

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

1,523,373

- Во Оценката на ЕУ за 2018, во врска со поглавјата 10 и 24 се вели дека Косово* бележи многу позитивен напредок во областа на информатичката безбедност и има многу добра законска регулатива. Сепак, најголемото прашање се однесува на спроведувањето, кое сè уште не го има достигнато потребното ниво

- Владата назначи 24/7 контакт центар во полициската единица за компјутерски криминал

- Најчестиот тип на компјутерски криминал вклучува измама со кредитни картички, лажни вести (на пр. фалсификувани е-пораки до медиумите), компјутерски напад, DDoS напади, fishing, итн.

- Односите меѓу јавниот и приватниот сектор се добри, особено кон интернет-провајдерите. Сепак, соработката сè уште не е на потребното ниво

ИНФОРМАТИЧКА БЕЗБЕДНОСТ

ОНЛАЈН РАДИКАЛИЗАЦИЈ А

- Интернет-содржини на албански јазик, во продукција на ИСИС, се наменети за албански говорници во Албанија, Косово* и во Поранешната Југословенска Република Македонија, но со посебен акцент на контекстот на Косово*

- Покрај значајната улога на социјалните медиуми, голем број извештаи за активности поврзани со ИСИС во Косово* ја споменуваат важноста на традиционалните масовни медиуми во процесите на радикализација и регрутирање

- Интернетот одигра значајна улога во процесите на радикализација на „странски борци“ на Косово

ЦРНА ГОРА

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

439,624

Статистика по година и тип на напад

	НАПАДИ НА ВЕБ-СТРАНИЦИ И ИСИС	ОНЛАЈН ИЗМАМИ	ЗЛОУПОТРЕБА НА ПРОФИЛИ НА СОЦИЈАЛНИ МРЕЖИ	НЕАДЕКВАТНИ ОНЛАЈН СОДРЖИНИ	ЗЛОНАМЕРЕН СОФТВЕР MALWARE	ДРУГО
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 (до 1 септември)	90	13	25	4	245	8
Вкупно	124	59	128	42	313	78

385
регистрирани сајбер-напади во 2017 година

- Во Оценката на ЕУ 2018, во врска со поглавјата 10 и 24, се вели дека Црна Гора не внесе суштинска евалуација во однос на информатиката и информатичката безбедност
- Во 2017 година, владата го формираше Советот за информатичка безбедност
- Приватниот сектор во Црна Гора е многу прогресивен во полето на информатичката безбедност, при што некои од давателите на ИТ услуги веќе 15 години функционираат како пионери во оваа област
- Црна Гора брзо напредува во областа на информатичката безбедност, од законодавна и политичка перспектива

ИНФОРМАТИЧКА БЕЗБЕДНОСТ

ОНЛАЈН РАДИКАЛИЗАЦИЈА

#3

Во Црна Гора постојат три главни видови на екстремизам:

- насилен такфиризам (во овој извештај „насилен џихадизам“)
- ненасилен салафизам
- и панславизам и православен екстремизам

Во врска со последниот тип екстремизам, има Црногорци кои му се приклучија на странскиот борбен контингент во Источна Украина

Поединечен преглед за секоја од земјите на Западен Балкан 6

СРБИЈА

ИНТЕРНЕТ- КОРИСНИЦИ ВО ДЕКЕМВРИ 2017 ГОД.

6,325,816

- Во Оценката на ЕУ 2018, во врска со поглавјата 10 и 24, се вели дека Србија допрва треба да усвои стратегија за компјутерски криминал
- CSIRT има ограничена функционалност поради кадровски проблеми
- Националниот CSIRT се наоѓа во Републичката агенција за електронски комуникации и поштенски услуги, но во Србија постојат и голем број други CSIRTs
- Има специјално обвинителство за борба против компјутерскиот криминал
- Областа на информатичката безбедност се смета за релативно ново поле на внимание на владата, за кое се смета дека е нов безбедносен предизвик
- Во најголем дел постои добра соработка помеѓу приватниот сектор и владата, и се подобрува

ИНФОРМАТИЧКА БЕЗБЕДНОСТ

20
регистрирани компјутерски напади во 2017 год.

SPAM

- Резултатите од истражувањето, спроведено кај младите од Санџак, покажаа дека повеќе од половина од испитаниците (52,6%) ги сметаат онлајн платформите како клучни за ширење екстремистички ставови и содржини
- Речиси половина од испитаниците (46,7%) во истото истражување мислат дека, во смисла на онлајн ширење, платформите за социјални медиуми се најважната алатка за екстремистичката пропаганда
- Значително помал број на испитаници сметаат дека „религиозните објекти“ се оние што имаат важност за ширење на екстремистички (7,1%) или дека таквите пораки биле широко распространети „во заедницата“ (8,3%)
- Во 2017 година, BIRN[3] изнајде повеќе од 30 веб-страници на екстремната десница на српски јазик

ОНЛАЈН РАДИКАЛИЗАЦИЈА

[3] BIRN – Balkan Investigative Reporting Network

НОВО ВИРТУЕЛНО БОЈНО ПОЛЕ
Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?
RegionalCooperationCouncil

Препораки за подобрување на информатичката безбедност

Национално ниво

- Развивање на рентабилни стратегии за ефикасност на трошоците и акциски планови уште во процесот на планирање и зајакнување на таквите планови со наменски резервирани средства
- Креирање и/или подобрување на известувачки структури за информатички инциденти
- Подигнување на свеста
- Користење на постоечките специјализирани знаења преку создавање мрежи на заинтересирани страни
- Идентификување и развивање на јавно-приватни партнерства (ППП) и градење на синергии
- Преглед на образовниот пристап кон ИКТ и информатичката безбедност

Регионално ниво

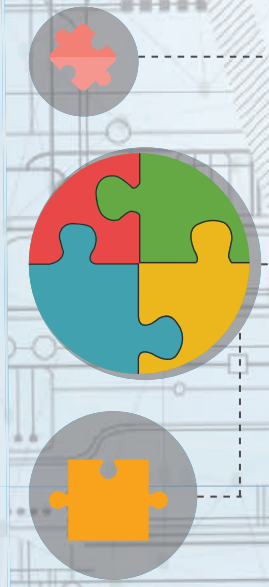
- Развивање на постратешки пристап кон регионалната соработка, во веќе постојните рамки
- Прилагодување/адаптирање на поддршката на меѓународната заедница за стратегијата на регионот
- Воспоставување на регионален центар за квалитет

Препораки за спречување на онлајн радикализам

Национално ниво

- Ревидирање на стратегиите за борба против насилен екстремизам (CVE) за да се обезбеди поголема усогласеност со Стратегијата на ЕУ за борба против радикализацијата и регрутирање за терористички цели
- Ревидирање на стратегиите за борба против тероризмот и насилниот екстремизам (CT and CVE) за да се обезбеди конзистентност и комплементарност со стратегиите за информатичка безбедност
- Ревидирање на стратегии и закони во доменот на борбата против тероризмот (CT) за да се обезбеди дека во нив се третираат напади врз информатичките системи
- Ревидирање на актуелните односи со компаниите од приватниот сектор, организациите на граѓанското општество и медиумите во правец на развивање на конкретни активности за нивно подобрување
- Преглед и развивање на одговори за решавање на општествените прашања кои групи или поединци може да се обидат да ги искористат за да добијат лична поддршка
- Спроведување на критичко размислување во образованието за информатичката безбедност

Регионално ниво



- Обезбедување конзистентен пристап кон екстремизмот и екстремистички содржини онлајн
- Практикување на пристап заснован на разузнавачки податоци и докази за да пристапувањето кон терористичките содржини се направи колку што е можно потешко и поскапо
- Развивање подобри односи со големите технолошки компании и КТ форуми
- Воспоставување на единица на земјите на Западен Балкан за постапување во случаи на пријавени интернет содржини
- Развивање и усвојување на агенда за безбедност на Западен Балкан
- Развивање на западно-балканска верзија на Мрежата за подигнување на свеста за радикализација на Западен Балкан

НОВО ВИРТУЕЛНО БОЈНО ПОЛЕ
Како да се спречи онлајн радикализација во областа на информатичката безбедност во земјите на Западен Балкан?
RegionalCooperationCouncil

10

YEARS

Powered
by RCC.int

СОВЕТОТ ЗА РЕГИОНАЛНА СОРАБОТКА

Трг Босне и Херцеговине 1/V

71000 Сарајево, Босна и Херцеговина

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

rcc.int RegionalCooperationCouncil @rccint RCCSec Regional Cooperation Council

RegionalCooperationCouncil