A NEW VIRTUAL battlefield

How to prevent online radicalisation in the cyber security realm of the Western Balkans?

Summary of the Study on Cyber Security (and Online Radicalisation) in the Western Balkans

RegionalCooperationCouncil

Good.
Better.
Regional.

funded by the EU

This publication is funded by the EU. It reflects only the views of the author(s). The Regional Cooperation Council and the EU cannot be held responsible for any use which may be made of the information contained herein.

RegionalCooperationCouncil

This **brochure** is **based** on the **study on cyber security (and online radicalisation) in the Western Balkans**, commissioned by the Regional Cooperation Council, within the IPA II 2016 Regional Action on P/CVE in the Western Balkans.

The main **objective** of the Study this brochure is based on is to provide a **comprehensive overview** and **analysis** of the situation regarding **cyber security** and **online radicalisation** in Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, Serbia, and The Former Yugoslav Republic of Macedonia (**Western Balkans 6** or WB6), and to **provide recommendations** for **enhancement of cyber security** and **prevention of online radicalisation**.

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of independence.

RegionalCooperationCouncil

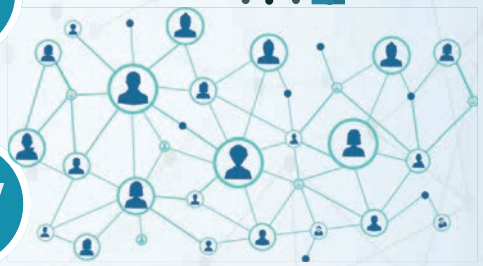
Global online environment overview

2015

2 Billion
number of internet users in 2015

2.28 Billion
number of social media users in 2016 worldwide

2016



3.8 Billion
number of internet users globally in 2017
or

51%
of world population

2017

2022

6 Billion
expected number of internet users by 2022

7.6 Billion
is expected growth of internet users by 2030

2030

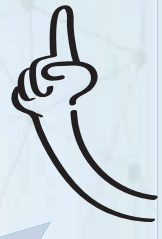
90%
of the world's 6+ y/o population will be using internet

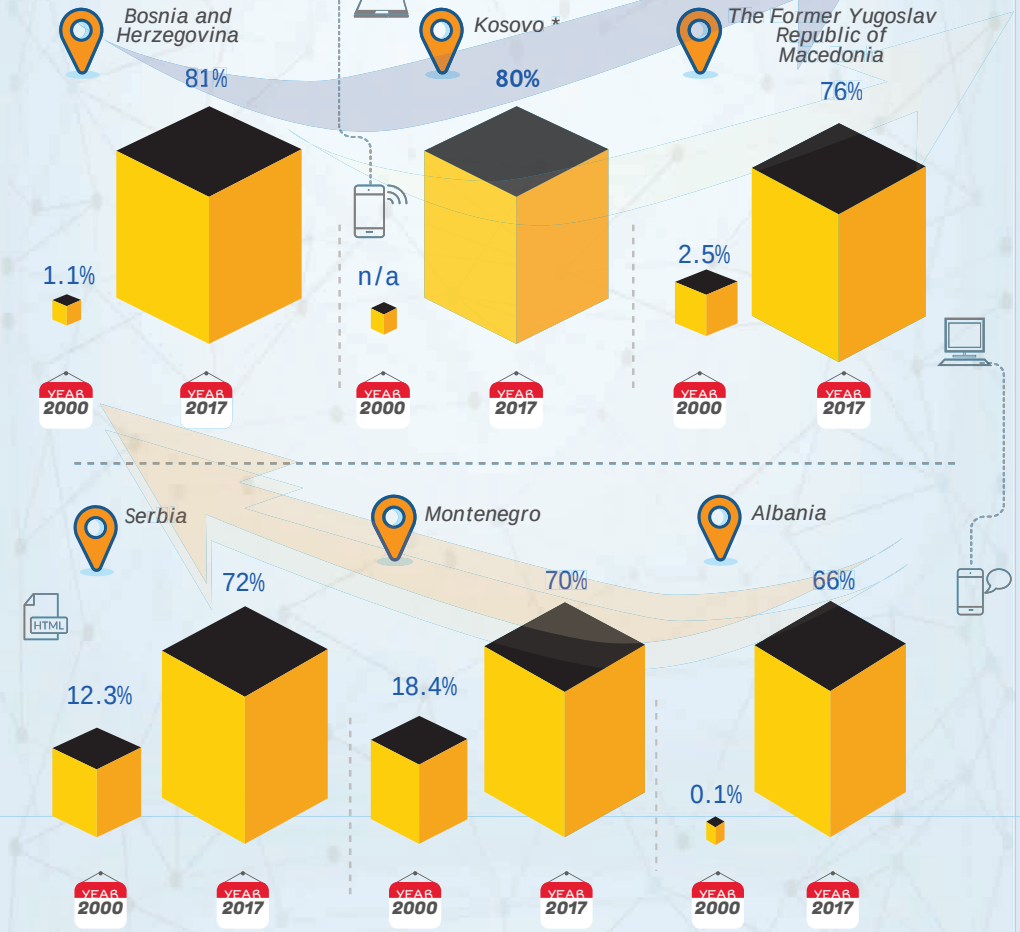
Regional online environment overview

% of internet users in the region:

IMPORTANT POINT!

Significant **growth** recorded in **internet use** in the **Western Balkans** between 2000 and 2017, with the number of **internet users** ranging from **66% to 81% of the population.**



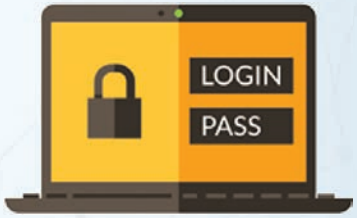


A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

Cyber Security

Contemporary **conceptions** of **cyber security,** which largely focus on **hard or kinetic attacks**, such as cyber-attacks and cybercrime, and omit **online information operations**, such as online radicalisation, hate speech and 'fake news', no longer fit the purpose.

A New Virtual Battlefield - How to prevent online radicalisation in the cyber security realm of the Western Balkans ambitiously **expands** our **understanding of cyber security** to **encompass both**, stemming from a growing **awareness by the RCC** that the **role of the internet** in information operations cannot and **should not** be viewed in **isolation** from **other areas** of **cyber security.**



How ready is the region for this approach?

Cyber Security

2015 Eurobarometer survey on **most common concerns of internet** users:

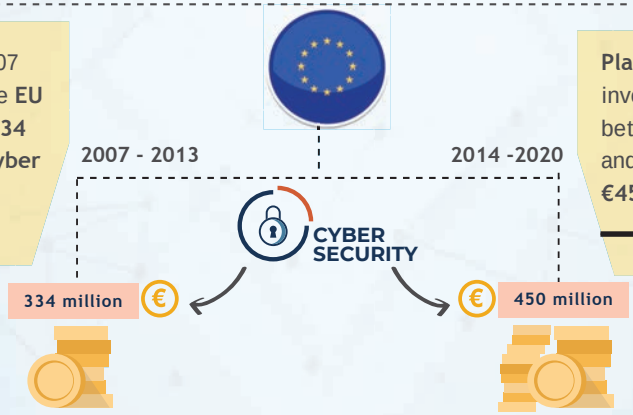
43% concerned about the misuse of their personal data

42% concerned about security of online payments

18% had no concerns about online banking or online payments

Between 2007 and 2013 the **EU invested €334 million** in **cyber security**

Planned further investments between 2014 and 2020 are **€450 million**



CSIRT

Computer Security Incident Response Teams (CSIRTs)

The functions of all the **Computer Security Incident Response Teams** (CSIRTs) in the **WB6** are very **similar;** however, their levels of **functionality** are **not consistent** across all economies.

None of the national **CSIRTs** in the WB6 are **standalone agencies,** but their positioning within governments is different across the region.

Cyber Security

Synopsis of relevant information and findings in respect to each of the WB6

	ALBANIA	BOSNIA AND HERZEGOVINA	KOSOVO*	THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	MONTENEGRO	SERBIA
Budapest Convention on Cybercrime	Ratified 2002 24/7 Point of Contact (POC)	Ratified 2006 24/7 POC	24/7 POC	Ratified 2004 24/7 POC	Ratified 2010 24/7 POC	Ratified 2009 24/7 POC
National CIRT	✓ 2016	Very limited functionality 2017	✓ 2016	✓ 2016	✓ 2012	✓ 2016
Law on Cyber Security	✓ Adopted 2017	✗	✓ Adopted 2010	✗	✓ Adopted 2010	✓ Adopted 2016
Cyber Security Strategy	Policy acts in lieu, 2015-2017	✗	Strategy and action plan 2016	Strategy Adopted in July 2018	Strategy and action plan 2018-2021 (2nd strat.)	Yes, no action plan 2017
3rd level education on Information Security	✗	✓	✓	✓	✓ multi-disciplinary	✗
CVE/Terrorism Strategy includes reference to cyber/online	✓	✓	✓	✓	✓	✓
Key Challenges	Technical, financial, expertise and accessing and retention staffing					

Regional challenges to implementation of Cyber Security Strategy

- CSIRTs: lack of financial investment commensurate with the required activity; lack of sufficient staffing; insufficient technological capacity
- Incident reporting: companies in particular fear reputational damage in case of media leaks; lack of confidence in law enforcement; lack of capacity to identify attacks when they happen
- Investigations and procedures: suffer from insufficient skills and capabilities
- Public private partnerships (PPP): lack of tradition of PPPs in the region; lack of demand for such initiatives; lack of recognition by governments of ICT experts within WB6 economies (preference for international experts)
- Education: apparent lack of educational policies focusing on ICT and related security in the WB6
- Media: noted lack of informed reporting on cyber security in the majority of the WB6
- Brain drain: high rates of migration of experienced ICT professionals from the region
- Lack of awareness of cyber security risks in the region

A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

Online Radicalisation

Violent extremists and terrorists...

...have, for some time, been **utilising the internet** to communicate, collaborate and convince which is exactly what the *Study on Cyber Security (and Online Radicalisation) in the Western Balkans* focuses on.

The **role of the internet** in **radicalisation** processes is **evident across the WB6**, but **personal interactions remain important.**

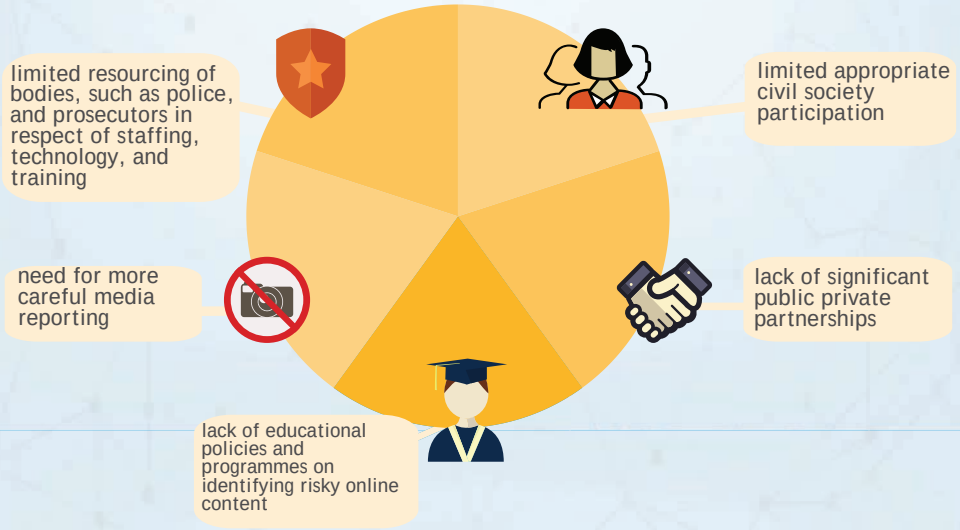
Critics of contemporary radicalisation discourse...

...claim that **'radicalisation'** is mostly associated with **violent jihadi** terrorism and is much less prevalent in discussions around **other types** of **violent extremism** and terrorism, such as the **extreme right**.

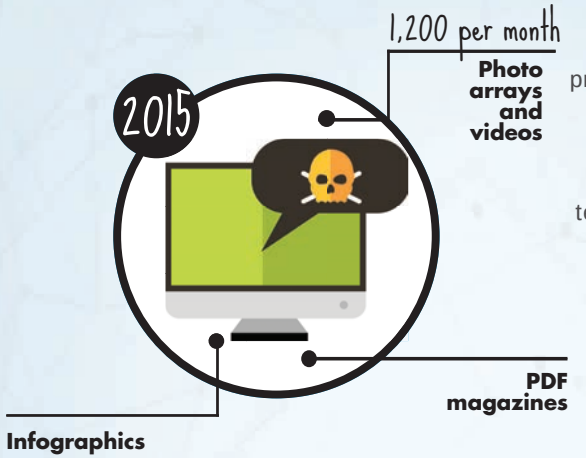
All but two WB6 have national-level strategies...

...for **countering radicalisation and/or violent extremism** – but **lag behind** in their **implementation.**

Most significant deficits associated with implementation of strategies for countering radicalisation:

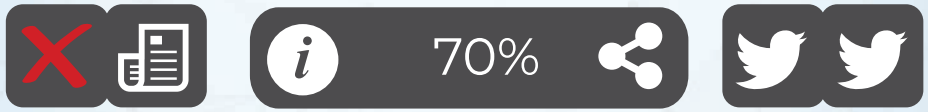


Online Radicalisation

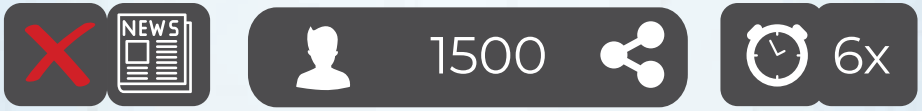


At the height of their online prowess in **2015**, Islamic State (IS) was producing approximately **1,200** items of official content monthly, including **photo arrays, infographics, PDF magazines, and videos.** IS are not the only terrorists active online, of course.

There are a variety of **violent extremists and terrorist groups** and their supporters currently engaged in a diversity of online activity.

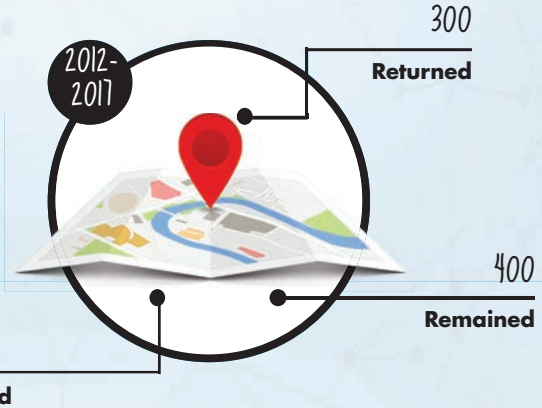


False info is 70% more likely to be retweeted than a true one



False story on average reaches 1,500 people 6 times quicker than a true story

In period 2012-2017 around **1,000** individuals (men, women, children, elderly) from the Western Balkans travelled to Syria and Iraq, out of whom around **300** returned, more than **200** were killed, some **400** remained, while some are considered missing.



A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

ALBANIA

INTERNET USERS IN DEC 2017

1,932,024

CYBERsecurity

- Does not have Cyber Security Strategy *per se*, but the Paper on Cyber Security 2015 – 2017 suffices in its absence
- Dedicated cybercrime units exist in State Police and General Prosecutor's Office
- EU Assessment 2018 for Chapters 10 and 24 says Albania is moderately prepared for information security, and some progress had been made in relation to the digital agenda action plan and e-government services
- Majority of cybercrime cases relate to fraud, hacking, online stalking, and data interference

ONLINE radicalisation

- Dissemination of extremist messaging has taken place through direct communication in about 70% of cases and about 30% via the Internet
- Social media are **not** the most important channel of dissemination of 'extremists' content in Albania

Overview per each of the WB6 - Cyber Security and Online radicalisation

BOSNIA AND HERZEGOVINA

INTERNET USERS IN DEC 2017

2,828,846

- EU Assessment 2018 for Chapters 10 and 24 says Bosnia and Herzegovina lacks a strategic [state level] framework to address the issue of cybercrime and cyber security threats. Investigations in cybercrime reportedly remain very rare.
- Main types of cybercrime include DoS*[1]* and DDos*[2]* attacks, internet fraud, unauthorised access to computer systems, credit card scams, wireless network abuse, online child sex abuse-related activity, online intellectual property rights violations, social network abuse, distribution of malware, inciting hatred, discord or intolerance, and public incitement to terrorism and terrorist propaganda
- There is no culture of information security in BiH yet – lack of awareness and understanding of potential impacts

CYBERsecurity

ONLINE radicalisation

- The Internet widely recognised as having facilitated the establishment and spread of a wide variety of transnational networks, including Salafi and jihadi networks. Large BiH diaspora, with notable Salafi contingents in Austria, Germany, the Netherlands, Slovenia, and Sweden, is connected via the Internet
- However, community ties and face-to-face contacts were more consequential
- A role for the internet in the increased nationalist rhetoric apparent in BiH has also been mooted
- In 2017, BIRN located more than 60 websites based in the Western Balkans promoting the idea of ethnically pure nation states, neo-Nazism, violent homophobia and other radical right-wing policies

[1] In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet
[2] A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic

A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?

RegionalCooperationCouncil

THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA

INTERNET USERS IN DEC 2017
1,583,315

CYBERsecurity

- EU Assessment 2018 for Chapters 10 and 24 says Criminal Code of The Former Yugoslav Republic of Macedonia is broadly in line with EU standards, criminalising online child sex abuse and computer crime, amongst other crimes. Digitalisation of the economy is progressing fast
- Does not have an overarching law on cyber security, but cyber security strategy has been adopted in July 2018
- Established their national CSIRT in 2016
- The majority of cyber-attacks were of DoS and phishing types, but malware distribution is increasing albeit there is a lack of awareness by many users of this threat

recorded
75
cyber-attacks in 2017

ONLINE radicalisation

- Easy access to extremist and terrorist content via the Internet, especially social media

Overview per each of the WB6 - Cyber Security and Online radicalisation

KOSOVO *

INTERNET USERS IN DEC 2017
1,523,373

- EU Assessment 2018 for Chapters 10 and 24 says Kosovo* has made some very positive progress in cyber security domain and it has very good legislation. However, the biggest issue relates to implementation, which has not yet been done to the level required
- The government appointed a 24/7 contact point within the police's cybercrime unit
- The most common type of cybercrimes include credit card fraud, fake news (e.g. through forged e-mails to the media), computer intrusion, DDoS attacks, phishing, etc.
- Relations between the public and private sectors are good, especially in respect to internet service providers. However, cooperation is still not where it could be

CYBERsecurity

ONLINE radicalisation

- IS-produced Albanian-language online content targeted Albanian speakers in Albania, Kosovo*, and The Former Yugoslav Republic of Macedonia, but with a particular focus on the Kosovo* context
- In addition to significant role of social media, a number of reports on IS-related activity in Kosovo* mention the importance of traditional mass media in radicalisation and recruitment processes
- Internet played a significant part in Kosovo* foreign fighters' radicalisation processes

A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

MONTENEGRO

INTERNET USERS IN DEC 2017
439,624

	ATTACKS ON WEBSITES and IS	ONLINE FRAUD	ABUSE OF SOCIAL PROFILES	INAPPROPIRATE CONTENT ONLINE	MALWARE	OTHER
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 (until 1 Sept)	90	13	25	4	245	8
TOTAL	124	59	128	42	313	78

recorded **385** cyber-attacks in 2017

- EU Assessment 2018 for Chapters 10 and 24 says Montenegro did not include a substantive evaluation in relation to cyber and cyber security
- In 2017, the Government formed the Information Security Council
- Montenegro is progressing quickly in the area of cyber security from a legislative and policy perspective
- Private sector in Montenegro is very progressive in the cyber security field, with some IT service providers pioneering in this area for at least 15 years

CYBERsecurity

ONLINE radicalisation

#3 There are three main types of extremism in Montenegro:

- violent takfirism (termed in this report 'violent jihadism')
- non-violent Salafism
- and pan-Slavism and Orthodox extremism

In terms of the latter type, some Montenegrins have joined the foreign fighter contingent in eastern Ukraine.

Overview per each of the WB6 - Cyber Security and Online radicalisation

SERBIA

INTERNET USERS IN DEC 2017
6,325,816

- EU Assessment 2018 for Chapters 10 and 24 says Serbia had yet to adopt a strategy on cybercrime
- CSIRT is of limited functionality due to the staffing issues
- The national CSIRT is located in the Republic Agency for Electronic Communications and Postal Services but a number of other CSIRTs are also present in Serbia
- It has a Special Prosecution Office for the fight against cybercrime
- The area of information security is seen as a relatively new field of awareness for the Government, but one that is seen as a new security challenge
- Good cooperation exists between the private sector and government, for the most part, and it is improving

CYBERsecurity

SPAM

recorded **20** cyber-attacks in 2017

- The findings of a public opinion survey conducted among young people from Sandžak showed that more than half of respondents (52.6%) viewed online platforms as crucial for dissemination of extremist views and content
- Almost half of respondents (46.7%) in the same survey thought that, in terms of online dissemination, social media platforms were the most important tool for extremist propaganda
- Considerably lower numbers of respondents felt that important for the spread of extremist messaging were "religious objects" (7.1%) or that such messaging was widespread "in the community" (8.3%)
- In 2017, BIRN located 30-plus Serbian-language extreme right websites

ONLINE radicalisation

A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

Recommendations for improvement of Cyber Security

NATIONAL LEVEL

- Develop cost efficiency strategies and actions plans during the planning phase and reinforce such plans with dedicated funds
- Create and/or improve cyber incident reporting structures
- Raise awareness
- Leverage existing expertise by creating networks of interested parties
- Identify and develop Public Private Partnerships (PPP) and build synergies
- Review educational approach to ICT and Cyber Security

REGIONAL LEVEL

- Develop a more strategic approach to regional cooperation, within existing frameworks
- Realign support of the international community to the strategy of the region
- Establish a regional centre of excellence

Recommendations for improvement of Cyber Security

NATIONAL LEVEL

- ✓ Review CVE strategies to ensure greater alignment with the EU Strategy for Combating Radicalisation and Recruitment to Terrorism
- ✓ Review CT and CVE Strategies to ensure consistency and complementarity with Cyber Security Strategies
- ✓ Review strategies and legislation in the area of CT to ensure attacks on information systems are included
- ✓ Review current relationships with private sector companies, civil society organisations and the media to develop specific actions to improve same
- ✓ Review and develop responses to address societal issues that groups or individuals may try to capitalise on to gain support
- ✓ Implement critical thinking into cyber security education

REGIONAL LEVEL

- ✓ Ensure a consistent approach to extremism and extremist online content
- ✓ Take an intelligence and evidenced approach to make access to terrorist content as difficult and costly as possible
- ✓ Develop better relationships with major tech companies and CT forums
- ✓ Establish a Western Balkans Referral Unit
- ✓ Develop and adopt a Western Balkans Agenda on Security
- ✓ Develop a Western Balkan version of the Radicalisation Awareness Network

A NEW VIRTUAL BATTLEFIELD
How to prevent online radicalisation in the cyber security realm of the Western Balkans?
RegionalCooperationCouncil

10

YEARS

Powered
by RCC.int

Regional Cooperation Council Secretariat

Trg Bosne i Hercegovine 1/V

71000 Sarajevo, Bosnia and Herzegovina

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

rcc.int RegionalCooperationCouncil @rccint RCCSec Regional Cooperation Council

RegionalCooperationCouncil