INTERNET RADICALIZATION AND THE POSSIBILITY OF SPREADING RADICAL IDEAS AND MATERIALS ON THE DARK WEB

Marjan Nikolovski, PhD[1]
Davor Arsic, MSc
Faculty of Security – Skopje, University "St. Kliment Ohridski" in Bitola
North Macedonia

INTRODUCTION

Technological development in the last few decades has been in constant growth and improvement. Society cannot be imagined to function normally without the use of special tools and programs on the Internet platform. The Internet brings the world together, but only virtually. Various social networks such as Facebook, Instagram, Skype, Twitter enable quick and easy communication with people who are on the other side of the planet. With that, information spreads very quickly and easily, because the rate of internet users is very high. Extremist groups make very good use of these networks, especially for their purposes related to the recruitment and training of fighters, so that they can then go to various battlefields in the Middle East.

The danger of online radicalization used by terrorist networks poses a big problem for the security services because the very act of tracing their communication can be faked and thus the plot for a particular terrorist attack or extremist act remains undetected. With the development of internet platforms, the way of spreading radical ideas has changed, apart from personal contacts and the spread of radicalism in paramosques that are not sufficiently controlled by state institutions, radical ideologies have started to spread quickly and via the internet, of course at a high speed. Terrorist groups are also recruiting experts in the field of informatics in their ranks in order to encrypt the messages between themselves, not to leave any virtual traces and preferably hacker attacks on certain state institutions, all in order to show their readiness that they will always be one step ahead of the security-intelligence services and state anti-terrorism services.

Mark Sageman is very explicit in his statement that the Internet can promote another special phenomenon, namely the so-called "lonely persons". Sageman points out that it is a new direction that has not been considered much and should be given more attention. Regarding the role of the Internet as an incubator or accelerator of "lone wolves" as a phenomenon and occurrence, it is stated that the Internet is an effective means of communication for "lone wolves" because it provides them with a place and opportunity to receive radical materials, training manuals, and video materials. De facto, it enables direct contact in the community of like-minded people around the world, who can connect, radicalization and spread of extremist ideas are encouraged and various activities are carried out (Sageman, 2008).

1 davorarsikjku@yahoo.com

INTERNET AND ONLINE RADICALIZATION

Internet radicalization as a kind of hybrid threat represents a wide field of action for criminal and extremist groups. Easy access to the internet, data and information derived from it can pose a security threat. We use a small percentage of the Internet space to which we have simple access through several Internet tools and search engines, but there is also a dark web to which access is a little more difficult, but not impossible. It is accessed using special tools and networks such as the Tor browser.

Tor (an acronym for The Onion Router) is essentially a network that masks online traffic. Tor browser is an open-source platform managed by volunteers and, due to its onion routing, creates anonymity for users who access websites and servers through this network. The browser is often used legitimately by journalists and other users who need to protect their identities, for example, while investigating the opposition in a legal dispute, or researching competitors. In the simplest terms, Tor browser is a software that allows users to browse the internet with a relatively high degree of privacy. The network and browser take their name from the fact that they direct all web activity through several routers—called nodes—much like going through the layers of an onion, making it difficult to track and identify users.[2]

The dark web is a small, less accessible part of the deep web. Both share one thing in common: Neither can be found in search engine results. The main difference between them is in how their content is accessed. Deep web pages can be accessed by anyone with a standard web browser who knows the URL. In contrast, dark web pages require special software and knowledge of where to find the content.[3]

The dark web is a dangerous place, where drugs are bought and hitmen are hired, but it can also be a safe way to browse the web if privacy is seriously compromised. And thanks to the Tor browser, all of this is easy to do, a de facto breeding ground for radical Islamists and lone wolves.[4]

The dark web [5] is a term that refers to a collection of websites that exist only on an encrypted network and cannot be found by traditional search engines or opened by ordinary web browsers. Almost all dark web sites hide their identity using Tor tool/network.

Tor represents a network platform that makes certain actions of the Internet user invisible, that is, anonymous.

The Tor Project, Inc, became a 501(c)(3) nonprofit in 2006, but the idea of "onion routing" began in the mid-1990s. In the early 2000s, Roger Dingledine, a recent Massachusetts Institute of Technology (MIT) graduate, began working on an NRL onion routing project with Paul Syverson. To distinguish this original work at NRL from other onion routing efforts that were starting to pop up elsewhere, Roger called the project Tor, which stood for The Onion Routing. Nick Mathewson, a classmate of Roger's at MIT, joined the project soon after. By the end of 2003, the network had about a dozen volunteer nodes, mostly in the U.S., plus one in Germany.[6]

It helps to hide certain activities on the internet. When a certain website with questionable content is operating on the Internet using the Tor application, it is not possible to find out who is behind that page, nor who hosts and maintains its validity.

2 https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser
3 https://www.techtarget.com/whatis/definition/dark-web
4 wolves.https://www.wired.com/story/what-is-the-dark-web-how-to-access/
5 https://pcchip.hr/internet/korisne-aplikacije/vodic-kako-pristupiti-deep-webu-a-kako-darknetu-1-dio/
6 https://www.torproject.org/about/history/

The dark web is all that ordinary browsers cannot see due to certain unknown reasons, and the dark web is a part of the dark web where prohibited content is found, it is used for the training of terrorist groups, their encrypted exchange of information and mutual cooperation.[7]

For this, other tools are used to access the dark web. In it many materials for indoctrination and radicalization of individuals, ideas for carrying out terrorist attacks can be found.

Terrorist groups to implement their strategies use many tools on the Internet for mutual communication, and in most cases, these are encrypted messages with special codes to prevent the security services from entering their trail. In a Eurostat survey conducted in 2015, an analysis was made of the annual increase in new internet users in the EU.

In 2022, the internet was used mainly to communicate with others, sending/receiving e-mails (77%), instant messaging (72%), to find information about goods and services (70%), telephoning or video calls (66%) and watching internet streamed TV or videos (65%).

A majority of people also used the internet for reading online news sites/newspapers (64%), watching video content from commercial or sharing services (61%), banking (60%), participating in social networks (58%), and listening to music (54%). [8]

According to these data, we can agree with the theses of scientists and researchers about the use of the Internet for terrorist purposes, and further indicate that the Internet facilitates the process of radicalization, because it is available to a large number of people around the world, 24 hours a day and in this way, the flow of information is facilitated, that is, the Internet provides space for the spread of terrorist propaganda and extremist beliefs.

By searching one of the tools such as Google Chrome, one of the world's most famous search engines, one can get access to a huge number of written documents, video clips, instructions related to terrorism and extremism.

According to sources to Europol from 2013 to 2015 the following figures describe the situation with acts related to terrorism and violent extremism. (Europol)[9]

Table 1.

Year	**2013**	**2014**	**2015**
Number of individuals detained in the EU for terrorism-related offences	537	774	1077
Number of persons detained for jihadist terrorism	216	395	687
Number of convictions for terrorism	258	345	417
Number of acquittals due to terrorism	78	107	110

On publicly available browsers for using internet services, one can get access to a huge number of written documents, video clips, instructions related to terrorism and extremism.

In the texts and messages, the English language is used because of its prevalence. So, for example, if data and materials related to terrorism and criminal acts are searched for on the Google Chrome

7 Source: Boris Plavljanic - IT expert at the Zagreb software company DEKODE, an expert in Internet networks and a connoisseur of surface and dark Internet methods. (https://poslovnipuls.com/2024/02/26/karijere-boris-plavljanic-decode/)

8 https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20221215-2

9 The data is taken from the Europol website.

search engine, a large number of results will be obtained. Thus, searching for the following words yields these results:[10]

1) "How to make a bomb?" or "How do I make an explosive device?" has 462,000,000 views.
2) "How to make da suicide belt!" or "How to make a suicide belt!" has 19,200,000 views.
3) "Islamic state" has 362,000,000 views.
4) "Jihadists" or "Jihadist" has 5,100,000 views.
5) "Beheading videos" - video materials whose content is the beheading of innocent victims, a method used by terrorists to intimidate and send a message that contains fear and panic to ordinary citizens and has 21,100,000 views.
6) "Who is Osama Bin Laden?" or "Who is Osama Bin Laden?" with 25,200,000 views.
7) "Who is Abu Bakr al-Baghdadi?" or "Who is Abu Bakr al-Baghdadi?" with 12,500,000 views.
8) "Wahhabism" or "Wahhabism" with 3,900,000 views.
9) "How to prepare a terrorist attack" or "How to prepare a terrorist attack" with 114,000,000 views.
10) "Training for terrorists"[11] or "Training for terrorist fighters" with 25,700,000 views. (Siqueira & Arce, 2020)

This data was obtained by searching the internet and these numbers refer to the day of the search, so the probability of being increased or decreased exists because new materials can be uploaded daily, and certain materials can be removed from the internet. These numbers are displayed by the search engine according to the words that are written, of course not all of these reviews actually contain such content, but of course it is enough that a certain percentage of the numbers contain radical materials that can be easily accessed every day, there is a great danger from this kind of radicalization.

Through the Internet platforms, easy communication between terrorist networks is carried out, propaganda is carried out, people who are easy to radicalize will enter the pre-radical phase very quickly with the help of this phenomenon. Such an example is seen in the documentary film of a Bosnian television called "Terrorist", where the parents of two young boys from Bosnia who have already left for the battlefields in Syria tell how the radicalization of their sons, who were exemplary children, began. The boys' mother said that members of a certain jihadist structure that operated in para-mosques outside the settlements, mostly in mountain villages, came to the boys' home and gave them CDs, certain materials with radical-extremist content. When asked by the boys' mother what the materials contained, they stated that they were songs, and did not contain any material with a radical-extremist ideology.

COMPARATIVE ANALYSIS AND SCOPE OF THE LEGAL REGULATION IN THE REPUBLIC OF NORTH MACEDONIA AND THE SURROUNDING COUNTRIES

In the Republic of North Macedonia, the Criminal Code includes some criminal acts that cover at least part of this problem. The problem with internet radicalization, as well as with any kind of spreading of hate speech, threats, and in the last period, the cynical mockery and humiliation of certain individuals on social networks, which led to the execution of suicidal acts and other illegal acts that are not criminal enough - legally incriminated.

10 Арсиќ, Д.,2021 „Странските борци повратници од боиштата од Блискиот Исток како безбедносна закана по Република Северна Македонија", Магистерски труд,.

11 https://www.sciencedirect.com/science/article/abs/pii/S0176268020300264?via%3Dihub

In chapter thirty-three, there is article 394-a[12] Terrorist organization, and further down in the criminal code is Dissemination of racist and xenophobic material through a computer system Article 394-d (1) Whoever disseminates racist and xenophobic written material to the public through a computer system, image or other representation of an idea or theory that aids, promotes or incites hatred, discrimination or violence, against any person or group, on the basis of race, color, national or ethnic origin, as well as religious belief, will be punished with imprisonment from one to five years. 168 (2) With the penalty from paragraph (1) of this article, the person who commits the crime through other means of public information will also be punished. (3) He who commits the crime from paragraphs (1) and (2) of this article by abusing his position or authority, or if due to those crimes there is disorder and violence against people or large-scale property damage, will be punished with imprisonment from one to ten years. (Criminal Code of the Republic of Moldova "Official Gazette of the Republic of North Macedonia" No. 37/96)

The crime of Terrorism, Article 394-b, is also included in the same chapter - and it only mentions as one sentence the destruction of public facilities, transport systems, infrastructure facilities, computer systems, which de facto and de jure is a very small scope of what they are can be used as a term for computer systems and whether only by destroying but also by abusing them leads to the degree of spreading of radical ideas as with the speed of light.

Article 251 of the CC of RSM Damage and unauthorized access to a computer system also mentions the damage to computer systems, unauthorized access to passwords, etc., but the possibility and danger of using the same computer systems for the spread of dangerous and radicalized information is not mentioned again. material that can be the basis for indoctrinating easy target individuals or the known lone wolves who have no other choice but to use these platforms to prepare and train themselves to perform such actions.

In a comparative experience with the Republic of Serbia in this area of security research, one can come to the conclusion that the situation is similar. We will list in more detail the crimes that have elements of computer crime. In Chapter 27 of the Criminal Code of the Republic of Serbia,[13] there are the following more or less basically similar crimes: Damage to computer programs (Article 298), Computer sabotage (Article 299), Preparation and introduction of computer viruses (Article 300), Computer fraud (Article 301), Unauthorized access to computer systems (Article 302), Unauthorized use of a computer network (Article 304), ("The Official Gazette of the Republic of Serbia", no. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019), Public call to the commission of a crime of terrorism in Article 391a, Recruiting and training for the execution of terrorist acts in Article 391b, Financing of terrorism Article 393.

In Chapter 27 of the Criminal Code of the Republic of Serbia, there are several criminal acts that are related to the possibility of spreading radical ideas using the Internet. Here are included the crime of damage to computer data and programs in article 298, Computer sabotage article 299, Creation and spread of computer viruses article 300, Computer fraud article 301, Unauthorized access to computer systems article 302. Unauthorized use of computer systems article 304.[14]

Through the analysis of the criminal acts of the Criminal Code of the Republic of Serbia, it can be concluded that they include a wide range of illegal actions through which radical Islamists can spread

12 The Criminal Code ("Official Gazette of the Republic of Macedonia" number 37/96)

13 Criminal Code ("Official Gazette of RS", no. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019)

14 Criminal Code ("Official Gazette of RS", no. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019)

radicalization under the cover of others through softer actions. Through unauthorized access to certain computer systems to send messages of radicalism and Islamism.

The biggest problem for the state authorities is how to identify the channels through which Serbian citizens arrive at the world's battlefields, as well as those who organize it. In addition to undoubtedly personal contacts, social networks are also widely used in this sense, where profiles that directly or indirectly recruit participants in the conflict appear and disappear just as quickly, both in Iraq and Syria, and in Ukraine. Some cases of terrorist activity have shown the mobilizing effect that an attack can have on an international level and the significant influence of social networks on the radicalization of individuals. The Internet creates vast opportunities for building relationships with like-minded people around the world and creating an environment that encourages violence.[15]

It is believed that the recruiters were paid handsomely for this work and that the narratives they used to recruit young people to go to Syria were untrue and tailored to suit them. The main and most influential recruiting narrative was that one was not going to Syria to defend the Islamic State, to fight for their goals, but for the goals and defense of all Muslims. All Muslims were presented as victims of discrimination and oppression, and young people were called to defend them. The Internet was the main way, a platform to recruit and change the thinking of the youth. They were offered videos of discrimination against Muslims and violence against them, propaganda and appeals for help. This kind of narrative was particularly successful because, according to Islamic beliefs, Syria is the promised land, the place where the "struggle of truth against falsehood" will begin. Possibilities and needs of the community for deradicalization and reintegration processes.

In Novi Pazar, the most accepted tolerant understanding of Islam is "the existence of different schools of thought within Islam, with the understanding that the basic tenets of the faith are common to all". Radicalism occurs when all other opinions are excluded and only one is imposed. Exclusivity further leads only to extremism. Extremism is understood as any religious position that is exclusive, because from the point of view of faith it does not make sense, since one of the basic messages of Muhammad's teaching is that one should not be exclusive and extreme. There is also a story about two students from Novi Pazar in Saudi Arabia who reached such a level of exclusivity that they considered all Muslims in the world to be infidels. They said, "only you and I are believers." One day they quarreled and after that each of them considered himself the only remaining true Muslim in the world. This story illustrates the extent to which those radicalized in this way are exclusive and do not accept authority. In their experience, all extremists when they reach those stages no longer have a group they belong to and don't accept authority. Because of a small disagreement, they will turn against everyone else.[16]

Mainly in the criminal code of the Republic of North Macedonia and the Republic of Serbia, the part where these negative phenomena are covered are similar, and both codes lack incriminations in the sense that recruiting, writing on social networks as a means of communication can be a potential security threat. Online radicalization itself is an insufficiently controlled method used by terrorist and extremist groups around the world.

There are several risk factors that have an impact on the emergence and implementation of online radicalization. Access to the Internet and its contents on a large scale is cited as the main motive. The weak institutional control over what and how is written and what materials are implemented and shared on social networks. Determining the reasons or motives that lead to radicalization according to

15 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.helsinki.org.rs/serbian/doc/Uspon%20desnice%20-%20slucaj%20Srbija.pdf

16 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.helsinki.org.rs/serbian/doc/Uspon%20desnice%20-%20slucaj%20Srbija.pdf

(Haji-Yenev 2021): Political goals (for example: changing the form of government, such as abolishing the democratic system with elections as we have now and introducing a dictatorship); Social goals (for example: how fans of a sports club try to make a change or achieve a goal – to convince fans from other clubs to support their club); Religious goals (for example: how members of a religion want to impose a change that will make their religion dominant and exclusive).

The process of online indoctrination often occurs through conversation (chats), persuasion, influence, affection or lectures organized in closed or isolated groups, forums, special rooms. Gathered through online newspapers, blogs, services and chat rooms, participants enter the forums where extremist ideology is self-reinforcing. (Shan and Phillips 2021)

As examples of online radicalization and the spread of extremist ideas and propaganda, we can cite the example of ISIS. ISIS had the ability to create a global network or brand to spread its ideology and message and thereby mobilize over 30,000 foreign fighters around the world could not have materialized if proper access and opportunities offered by the internet were not provided.

The following five roles that the Internet plays in promoting radicalization can be identified: (i) the Internet creates more opportunities for radicalization; (ii) the Internet acts as an "echo chamber"; (iii) the internet accelerates the radicalization process; (iv) the internet enables radicalization without physical contact; (v) the internet increases opportunities for self-radicalization. The younger generation is particularly vulnerable to online radicalization because they accept online media much more naturally as part of their lives and social relationships than older generations. This means that the importance of face-to-face communication is decreasing and contacts via the Internet face a lot of trust, making policy interventions towards increased security on the Internet a priority for every government. (Haji-Janev & Risteska & Shabani, 2021)

The Internet and its tools are also used as a propaganda tool using the power of the media and the spread of misinformation online. What will mark the current year 2024 is the influence of the extreme right in the elections in several countries of Western Europe. Of course, the influence of Russian Internet propaganda on the decisions of citizens from European countries is worth noting. These activities are in the context of the so-called "information warfare."

In that context we can mention the influence or interference in the 2016 US presidential election. Namely citizens of the Republic of North Macedonia were mentioned in the global media for the involvement of hackers from Veles city in helping the election of Donald Trump in the 2016 US presidential elections.

In the current year 2024, citizens of the Republic of North Macedonia were mentioned that with their malicious IT activities in the recent electoral processes in Venezuela.

The public prosecutor of Venezuela, Tarek William Saab, accused that certain individuals, IT experts from Macedonia, had influence in the recent election processes in Venezuela with illegal activities and illegal malicious breach in the Venezuelan information system. The prosecutor indicated on grounds of suspicion that the Venezuelan local opposition had cooperation with Macedonian hackers, during which attempts were made to manipulate the election results for the election of the president of Venezuela, which ended unsuccessfully.

The Venezuelan Attorney General has officially announced that an investigation has been launched into the hacking of the data transmission system of the National Electoral Council (CNE). A cy-

ber-attack coordinated by Macedonia was recorded with the aim of changing the election results in favor of the opposition.[17]

If the information about the involvement of persons belonging to the IT-underground from Macedonia in influencing the elections in Venezuela, the USA is confirmed, the possibility of their involvement in Internet propaganda against European citizens in the recent elections, as well as their connection with IT, is not excluded. - hackers from Russia, which should be the subject of research in the coming period.

Ukrainian President Zelensky's[18] call for all interested persons to join the battlefields throughout Ukraine after the Russian invasion in 2022 through an online form is a striking example of the online spread of extremist ideas and propaganda. Of course, this de jure is a crime in our legislation and any departure would be sanctioned by law.

Internet propaganda as a powerful tool of the great world powers was also used in the past to interfere in the domestic and state interests of certain countries. Such is the glaring example of Russia's meddling in the 2016 election, where the US National Security Service issued a report on Russian influence on young voters in the US.

The Internet Research Agency (IRA), based in St. Petersburg, Russia, created thousands of social media profiles it claimed were Americans who supported radical political groups and planned or promoted pro-Trump and anti-Clinton events. They reached millions of social media users between 2013 and 2017. Fabricated articles and disinformation were distributed by the Russian government-controlled media and promoted on social media. In addition, computer hackers linked to the Russian military intelligence service (GRU) infiltrated the information systems of the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and Clinton campaign officials, particularly Chairman John Podesta, and publicly released stolen files and emails during the election campaign that could damage the reputation of one of the candidates. Several individuals with ties to Russia contacted various Trump campaign associates, offering both business opportunities to the Trump Organization and providing damaging information about Clinton. Russian government officials have denied involvement in any of the hacking or leaking of information. Russian meddling activities prompted strong statements from US intelligence agencies, a direct warning from then-US President Barack Obama to Russian President Vladimir Putin, the reimposition of economic sanctions against Russia, the closure of Russian diplomatic facilities and the expulsion of their staff.

The Senate and House Intelligence Committees have conducted their own investigations into the matter. Trump has denied there was any interference, claiming it was a "hoax" perpetrated by the Democratic Party to explain away Clinton's loss.[19]

On April 25, 2024, the European Union passed a special resolution on the interference of the Russian Federation in the European Parliament elections held at the beginning of 2024. The document voted by the European Parliament analyzed the election process and made some conclusions regarding the interference in internal affairs by Russia and its partners.

The resolution of the European Union and the European Parliament adopted by 433 votes "for" 56 "no" with 18 abstentions the resolution on "Russiagate": allegations of Russian interference in the

17 The monitoring of communications and the manipulation of data have become a negative phenomenon in the IT underground in Macedonia, New Macedonia, 08/08/2024

18 https://www.theguardian.com/world/2022/feb/27/ukraine-appeals-for-foreign-volunteers-to-join-fight-against-russia

19 Hosenball, Mark (2020-08-19). Mohammed, Arshad, yp. „Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election". Reuters). Washington. 2021-09-05.

democratic processes of the European Union. The text adopted at the plenary session was submitted by EPP, S&D, Renew, Greens/EFA, ECR groups and members. The resolution states that there is evidence of Russian interference and manipulation in many democratic countries, as well as its practical support for extremist forces and radical-minded entities to promote destabilization of the Union. The Parliament's special committee on foreign interference in all EU democratic processes, including disinformation, has exposed in detail Russian-led efforts and operations to infiltrate, influence and interfere with European democracies and EU institutions. Although the European Parliament's response to foreign interference has become more cautious, the resolution stresses that stronger measures should be adopted to ensure effective protection against undue external influence. Internal reforms have yet to be undertaken and must be done, Russia has established contacts with parties, personalities and movements in order to rely on actors in the institutions of the Union in order to legitimize Russian positions, support independence movements and carry out pressure to ease sanctions and mitigate the consequences of international isolation. Members of certain political groups, as well as some non-affiliated members, spread blatant pro-Kremlin propaganda in Parliament. Furthermore, the Parliament unequivocally condemns the ongoing Russian efforts to abuse and falsify the historical memory of the most tragic periods in Europe, including the consequences of the Molotov-Ribbentrop Pact and the terror that followed for the territories conquered by Nazi Germany and Communist Russia, in order to make an attempt to justify its present brutal, illegal and inhumane aggression and its expansionist policy. It expresses deep concern over reports that MEP Tatyana Danoka may have acted as an informant for the Fifth Service of the Federal Security Service of the Russian Federation while also serving as a Member of the European Parliament. The resolution also points to other instances where members knowingly serve Russia's interests. It considers it imperative to immediately conduct a thorough internal investigation in order to assess all possible cases of foreign interference by Russia and other types of malicious interference in the work of the European Parliament. Parliament also expressed particular concern over recent reports that Russian .authorities are providing specific narratives to far-right political parties and actors in various EU countries, notably Germany and France, aimed at undermining public support for Ukraine, after the full invasion of Russia in 2022. Members are extremely concerned about the alleged relationship between Catalan secessionists and the Russian administration.[20]

In the context of the latest events in Vienna, where a major terrorist act was prevented, the thesis that using Internet applications spreads radical ideas is confirmed again. Arrested 19-year-old Muhammad at his home in the town of Ternitz in Lower Austria, where a terrorist attack was being planned during Taylor Swift's concerts in the Austrian capital. During the search of his home, chemical substances and technical devices were found, which are now being examined. He said he stole the chemicals from his former employer. A few weeks ago, he posted a video on TikTok swearing an oath to the Islamic State.

The American pop star Taylor Swift was supposed to perform in Vienna today, tomorrow and Saturday. The concerts were canceled yesterday due to serious security threats, which followed the arrest of Muhammed and another Austrian citizen.

The arrest of 19-year-old Muhammed of Macedonian origin, suspected of planning a terrorist attack on Taylor Swift's concerts, recalls the November 2020 terrorist attack, also in Vienna, when 20-year-old Kujtim Fejzulai, of Macedonian origin, killed four and injured 23 more people.[21]

20 Resolution adopted by the European Parliament 2024/2548(RSP); Resolution on Russiagate: allegations of Russian interference in the democratic processes of the European Union

21 https://sdk.mk/index.php/makedonija/avstrija-pobara-od-makedonskata-politsija-da-go-proveri-19-godishnikot-uapsen-za-planirane-teroristichki-napad-na-kontsertite-na-tejlor-svift/

In 2020, Fejzulai was killed by the police during the attack. Austrian police said that Fejzulai, born in Vienna, had both Austrian and Macedonian citizenship, and his parents were originally from Chelopek. He had never been to Macedonia. Police also said he was an Islamic State sympathizer who served several months in prison in 2019 for trying to leave to fight in Syria. Police confirmed that Fejzulai was released early from prison after undergoing a de-radicalization process.

In both cases, there is the use of the Internet as a method and way of preparing and training for committing terrorist acts. Using the TOR network, terrorists can exchange information and data on the methods of execution, on the method of financing terrorist attacks, and the same contacts cannot be detected by the security services.

The example of Wagner's group, who died in a helicopter accident a few months ago, was succeeded by his son Pavel Prigozhin, who also uses online methods and forms to apply for participation in a military hotbed.

In comparison with Kosovo and Metohija[22], in their criminal code there are several crimes that have elements of crimes related to the abuse of computer systems, but again the part of online radicalization, online recruitment of fighters and extremists is exempted. In Article 199[23] Violation of the secrecy of letters and computer databases, Article 327 Unauthorized entry into a computer system. In the same, there is a criminal section Harassment where in one article it is stated if the same thing happens through computer systems, but nothing of the possibility of online radicalization or recruitment. In Article 134 Incitement to commit terrorist acts, distribution, incitement, spread of radical ideology, but again without incriminating the possibility of online radicalization, online spread of that ideology through social networks. (Official Gazette of Kosovo / no. 2 / January 14, 2019, 1 code no. 06/l-074 Criminal Code of Kosovo)[24]

Again, the fact is missing that nowhere in the above-mentioned criminal legislations is mentioned the online spread of radical ideas, sensitive chats between extremists and new people who have yet to be indoctrinated. In Bosnia, indoctrination of young people with covert materials and electronic devices where false written content, such as the example with Toše's CD, and in fact, inside, the security forces of BiH found radical materials, propaganda, ways and methods of committing the crime of Terrorism.[25]

A study by Jens Binder and Chris Baker-Bill[26] from Nottingham Trent University in England highlights the danger of online radicalization that can lead to the commission of a terrorist act, namely in that study it is stated that a greater number of convicts who are convicted of certain crimes related

22 According to the Constitution of the Republic of Serbia Kosovo and Metohija is an autonomous region in Serbia. (Starting from the state tradition of the Serbian people and the equality of all citizens and ethnic communities in Serbia, starting from the fact that the Province of Kosovo and Metohija is an integral part of the territory of Serbia, that it has a position of essential autonomy within the sovereign state of Serbia and that from such a position of the Province of Kosovo and Metohija follows the constitutional obligations of all state bodies to represent and protect the state interests of Serbia in Kosovo and Metohija in all internal and external political relations, the citizens of Serbia bear).Source: Based on Article 133, paragraph 3 of the Constitution of the Republic of Serbia and Article 25 of the Law on Referendum and People's Initiative ("Official Gazette of RS", no. 48/94 and 11/98)

23 The Official Gazette of the Republic of Kosovo / no. 2 / January 14, 2019, Pristina 1 law no. 06/l-074 Criminal Code of the Republic of Kosovo.

24 Based on Article 142, paragraph 2 of the Constitution of the Republic of Serbia and Article 25 of the Law on Referendum and People's Initiative ("The Official Gazette of the Republic of Serbia", No. 48/94 and 11/98), the Republic of Serbia has an autonomous province of Vojvodina and an autonomous province of Kosovo and Metohija. The essential autonomy of the Autonomous Province of Kosovo and Metohija will be regulated by a special law adopted according to the procedure provided for amending the Constitution.

25 https://www.capital.ba/teroristi-se-preselili-na-internet-da-vrbuju-i-sire-propagandu/

26 https://theconversation.com/terrorist-recruitment-now-happens-mainly-online-which-makes-offenders-easier-to-catch-196313

to terrorism, training and financing of terrorism were online radicalized, that is, without any offline interactions, but only online contacts and the spread of radicalism.

The radical preacher Anwar al-Awlaki often positioned himself as a propagandist who could motivate Western audiences for a generation of young Western Muslims who sought easy answers to complex questions (often via the Internet), Awlaki helped find a way for the global jihad movement to make it appealed to many who might otherwise have been beyond its ideological reach. In the early 2010s, the main security threat turned to IS. As noted above, over 50,000 individuals traveled to join the group, with IS planning and inspiring hundreds of attacks. In addition, the group has maintained a strong social media presence estimated to have at least 46,000 pro-ISIS Twitter accounts and thousands of foreign terrorist fighters who have participated in various battlefields and often with the help of ISIS supporters who spread radical material online.[27]

This mobilization, combined with the group's social media reach and slick propaganda, has led to widespread concern about the Internet's role in radicalization – UN Security Council Resolution 2178 explicitly requires states to take steps to address this threat and expressed concern about the role of the Internet "in encouraging others to commit acts of terrorism" (United Nations Security Council 2014).

While IS has occupied the headlines around the world, the threat from violent right-wing extremists has not gone away and has seen a strong resurgence in recent years, especially in the context of the internet. Several terrorist attacks in the past five years in which the Internet played an important role, including the 2017 Charlottesville drive-in attack; and attacks in Christchurch, El Paso and Halle in 2019, Buffalo and Bratislava in 2022.[28]

This research uses detailed risk assessment reports for people convicted of terrorism offenses in England and Wales, based on 437 cases between October 2010 and December 2021. These reports are written by trained professionals in their field. The results of this research showed that, over time, people become less and less radicalized offline, such as in certain locations and meeting places or through direct contact with peers and relatives. Mixed radicalization, where extremist offenders are subject to both online and in-person influences, is also declining. It is now much more common for people to become radicalized online. They may learn from online sources or engage with extreme views on social media. They may also use Internet forums and chat groups that provide easy access to other like-minded people. These findings show that despite current perceptions of the growth of encrypted messaging services, online radicalization does not necessarily occur predominantly through one-to-one communication channels. The most commonly named platform is YouTube.[29]

CONCLUSIONS AND RECOMMENDATIONS

In the last years of the technological development of society, the ways of communication have also developed, the speed of information exchange is increasing and the overall way of functioning of the

27 This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu). Luxembourg: Publications Office of the European Union, 2022

28 This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu). Luxembourg: Publications Office of the European Union, 2022

29 https://theconversation.com/terrorist-recruitment-now-happens-mainly-online-which-makes-offenders-easier-to-catch-196313

social order is taking a new direction. Today, human existence cannot be imagined without the use of Internet platforms, in a word, everything is connected with electronic communications and the Internet. In the last 2 decades after the big terrorist attack in the USA, the world continued in another dimension and with questions that the authorities had to answer before their citizens. Even then, in that terrorist attack, information about the possible encrypted messages between the terrorists was spread in the media to reduce the chances of their detection. Internet radicalization on the dark web is a potential target for terrorist networks in the future. Ways, means and methods of how to quickly spread the radical idea, what plans are in the future, and how an application for participation in some foreign military hotspots can be filled out and sent through a simple online form.

The Internet is used as a propaganda tool and certain groups use it to hack and interfere in the internal affairs of their opponents. Interfering in election cycles as the most democratic right of citizens is a flagrant violation of international law and its regulations, but also a violation of democracy and human rights and freedoms.

Internet radicalization will continue to pose a danger and security threat to the normal functioning of society in the future. The large number of war hotspots around the world, in recent years with the Russian invasion of Ukraine, the attacks in Gaza by the Israeli army on Hamas are possible potential cells for the activation of certain terrorist groups, which have and will include individuals for online spreading their ideologies and ideas for action.

Technological advances have opened new channels for extremist organizations to spread their messages and win support for their political goals. This tendency can also be observed in the Western Balkans (WB). In addition to facilitating communication between individuals, social networking platforms have also facilitated the spread of hateful voices and extremist views. Extremist organizations have mastered the use of the Internet to spread their radicalism ideology and find supporters for their goals. (Dukić, 2021)

High school students are very dependent on their classmates for a sense of well-being, needing to feel part of a group, but also to be perceived as unique, and their currency is likes and ratings. CIKP's core study "Transition to Prevention: Using Education to Prevent Online Radicalization Among Youth" provides additional findings for high school students in Gostivar, Kumanovo, Skopje, Shtip, Tetovo and Veles, noting that 99% of students have access to the Internet in their homes, of which 85% said that they have access at any time, but also that in 74.4% of homes there are no rules for using the internet. Almost half of the students would accept parental control (44.1%), while more than half (55.9%) of the students think that parental supervision or control is necessary.[30]

The European Commission in its document entitled Radicalization Awareness Network (ec.europa.eu/ran) lists several main points related to online radicalization on the Internet:

- Extremist ideologies are not limited to the influence of one state,
- The Western Balkans is very susceptible to the spread of misinformation and fake news,
- The region of WB still endures the aftermath of previous wars in the former SFRY.[31]

As possible recommendations, greater international cooperation in the area of the internet and online radicalization can be mentioned, in the form of preventive action and prevention of the spread of radicalism on the internet. Threats from online radicalization do not represent a single threat only for one

30 Study on young people in North Macedonia 2018/2019, Friedrich Ebert Foundation, p.16 available at: http://library.fes.de/pdf-files/id-moe/15266.pdf

31 https://home-affairs.ec.europa.eu/document/download/1cca4520-3c96-42f2-adb4-2d1cb26e9611_en?filename=ran_paper_online_radicalisation_p-cve_approaches_in_wb_16062022_rs.pdf

territory or only for one country, the danger from it can affect both regional and international levels. The factor of cooperation between institutions, young people and especially those who are vulnerable to extremism and radicalism is very important. Non-governmental institutions can play an important role in the chain of preventive measures to prevent the spread of radical ideas on Internet platforms. Important recommendations are the organization of forums, lectures and training of young people to recognize such a danger and to inform the competent authorities about it.

To introduce experts from the field of security and criminology in primary and secondary schools in order to hold briefings, trainings and trainings of a practical nature on how to recognize an attempt at online radicalization. In the amendments to the Criminal Code itself, an amendment can be proposed by inserting a new article/paragraph in the Criminal Code with the name online radicalization or online spreading of extremist and radical ideas that conflict with normal social life.

LGUs in cooperation with government bodies and non-governmental organizations to organize training workshops for the most vulnerable groups of the population, especially the young generation which is a soft target and there is a danger of future radicalization by radical and extremist groups, in order to present the danger that it brings internet radicalization, suspicious profiles on social networks that can be a choice of radical ideologies.

REFERENCES

Арсиќ, Д.,2021 „Странските борци повратници од боиштата од Блискиот Исток како безбедносна закана по Република Северна Македонија“, Магистерски труд,.

Dukic, S. (2021). Ekstremizmot na internet vo RSM - Politika, etnicka pripadnost i religija. Mreza na silni gradovi, Institut za strateski dijalog

Sageman, M., 2008„Leaderless Jihad“, Philadelphia, University of Pennsylvania, press , str.12

Siquera, K& Arce, D. 2020, European Journal of Political Economy Volume 63, June 2020, 101878

Shan and Phillips (2021)

Hadzi,Janev,M & Risteska,M & Sabani,S , Skopje, 2021Response to Online Radicalization: Towards On-line Safety Education Policy Evropol

https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20221215-2

https://www.sciencedirect.com/science/article/abs/pii/S0176268020300264?via%3Dihub

The Criminal Code ("Official Gazette of the Republic of Macedonia" number 37/96)

Criminal Code ("Official Gazette of RS", no. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019)

https://www.theguardian.com/world/2022/feb/27/ukraine-appeals-for-foreign-volunteers-to-join-fight-against-russia

Official Gazette of the Republic of Kosovo / no. 2 / January 14, 2019, Pristina 1 law no. 06/l-074 Criminal Code of the Republic of Kosovo

https://www.capital.ba/teroristi-se-preselili-na-internet-da-vrbuju-i-sire-propagandu/

https://theconversation.com/terrorist-recruitment-now-happens-mainly-online-which-makes-offenders-easier-to-catch-196313

https://theconversation.com/terrorist-recruitment-now-happens-mainly-online-which-makes-offenders-easier-to-catch-196313

https://www.torproject.org/about/history/

https://www.wired.com/story/what-is-the-dark-web-how-to-access/

https://pcchip.hr/internet/korisne-aplikacije/vodic-kako-pristupiti-deep-webu-a-kako-darknetu-1-dio/

https://www.techtarget.com/whatis/definition/dark-web

https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser

Извор:Борис Плављаниќ-ИТ експерт во Загребачка софтверска компанија ДЕКОДЕ, експерт за интернет мрежи и познавач на методите за површински и темен интернет.(https://poslovnipuls.com/2024/02/26/karijere-boris-plavljanic-decode/)

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.helsinki.org.rs/serbian/doc/Uspon%20desnice%20-%20slucaj%20Srbija.pdf

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.helsinki.org.rs/serbian/doc/Uspon%20desnice%20-%20slucaj%20Srbija.pdf

Следењето на комуникациите и манипулацијата со податоците станаа негативна појава во ИТ-подземјето во МАкеоднија, Нова Македонија, 08.08.2024 година

Hosenball, Mark (2020-08-19). Mohammed, Arshad, ур. „Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election". Reuters). Washington. 2021-09-05.

Резолуција донесена од страна на Европскиот парламент 2024/2548(RSP)

Resolution on Russiagate: allegations of Russian interference in the democratic processes of the European Union

https://sdk.mk/index.php/makedonija/avstrija-pobara-od-makedonskata-politsija-da-go-proveri-19-go-dishnikot-uapsen-za-planirane-teroristichki-napad-na-kontsertite-na-tejlor-svift/

Устав на Република Србија член 133, став 3 и член 25 од Законот за референдум и народна иницијатива („Службен весник на РС", бр. 48/94 и 11/98)

Устав на Република Србија 142, став 2 и член 25 од Законот за референдум и народна иницијатива („Службен весник на РС", бр. 48/94 и 11/98),

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu). Luxembourg: Publications Office of the European Union, 2022