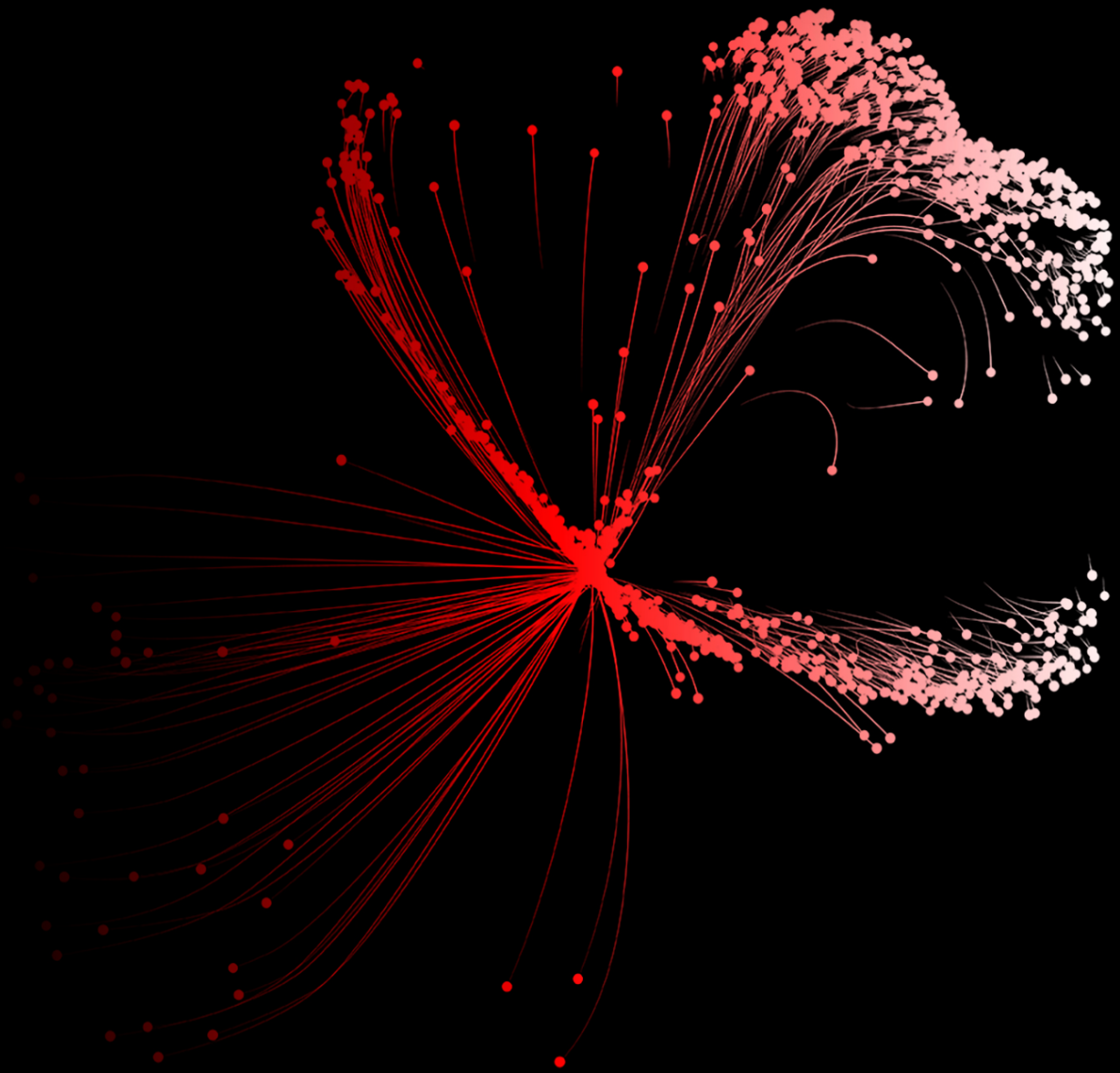
Funded by
the European Union

SOCIAL
JUSTICE
CENTER

ONLINE RADICALIZATION
AND WAYS TO COUNTERACT ITS IMPACT



Funded by the European Union

SOCIAL JUSTICE CENTER

GEORGIAN YOUNG LAWYERS' ASSOCIATION

CRRC GEORGIA | CAUCASUS RESEARCH RESOURCE CENTER

This publication has been produced with the assistance of the European Union, within the project "Supporting Accountable and Human Rights-oriented Security Sector through Research, Advocacy and Inclusive Dialogue". Its contents are the sole responsibility of Social Justice Center and they do not necessarily reflect the views of the European Union.

Author: Gonzalo Croci

Cover: Salome Latsabidze

Citation: *Croci, G. (2024). Online Radicalization and Ways to Counteract its Impact. Social Justice Center.*

Address: Abashidze 12 b, Tbilisi, Georgia

Phone.: +995 032 2 23 37 06

www.socialjustice.org.ge

info@socialjustice.org.ge

https://www.facebook.com/socialjustice.org.ge

Online Radicalization and Ways to Counteract its Impact

Table of Contents

1. Introduction

The advantages of the internet, such as its accessibility, lack of restrictions, large potential audience, and rapid information flow, have been abused by organizations dedicated to radicalizing individuals to further their agendas. Radicalism implies a collection of attitudes or behaviours that include a desire to rebel against the political, social, and cultural systems as well as, more broadly, the accepted norms and practices in society (Galland, & Muxel, 2020). The routes by which individuals are being ideologically radicalized is evolving and is increasingly taking place within social media platforms and online communities. Radical groups have shown themselves to be adept users of social media technology since the early days of the internet, using the internet to produce and spread content, draw in and radicalize followers, plan online and offline operations, and generate income. As such, the internet has become one of the primary operational environments in which radical political ideologies are realized, attacks planned, and social movements made (Winter, Neumann, Meleagrou-Hitchens, Ranstorp, Vidino, & Fürst, 2020).

Several stakeholders, including governmental organizations, law enforcement agencies, the media, and others have emphasized the threat of online radicalization as a key policy issue (Correa & Sureka, 2013). Nowadays, the majority of high-priority national security investigations, intelligence, and law enforcement organizations include the internet. Violent and non-violent radical organizations have taken advantage of the changing information environment by using social media platforms and easily accessible information technology to reach a wider audience and recruit vulnerable individuals (Bastug, Douai, & Akca, 2020). This is particularly worrying, since research has shown that most individuals fail to discriminate between genuine, fraudulent, and misleading online content, which makes them vulnerable to accidentally spreading inflammatory or propagandistic materials (Williams, Evans, Ryan, Mueller, & Downing, 2021).

The literature shows that there are two fields that can feed radicalization, online and offline domains. However, the arbitrary separation has been challenged since radicalised individuals use both domains for their activities and they seamlessly move across the two (Pauwels & Schils, 2016; Gill et al., 2017; Whittaker, 2022). Furthermore, most scholars today agree that radicalization is not a linear or a step-by-step process, but rather a multifactorial phenomenon (Frissen, 2021), where different mechanisms operate in different ways for different people in different contexts (Borum, 2011). This report presents the main theories and ways radical groups influence and attract individuals online, and the most common tools and strategies governments use to counter its impact.

2. Radicalization: Theories and definitions

The term "radicalism" is older than "extremism", and its meaning has evolved over more than two centuries. The main difference between these two terms is that radicalism can be situated at the edges of the democratic consensus while extremism lies outside (Bötticher, 2017). Further, focusing on ideological radicalization runs the risk of equating radical ideals with terrorism, even if we are aware that this is untrue. Most radical individual do not commit acts of terrorism, and many terrorists lack radical ideological convictions and may not even "radicalize" in the conventional sense (Borum, 2011). It appears that although radicalization can lead to adopt extremist beliefs that justify violence and terrorist activity, it is only one of many possible pathways into terrorist involvement.

The idea of radicalization, according to Borum (2011), Sedgwick (2010), Schuurman and Taylor (2018) and others, is unclear, especially in terms of whether it refers to a process of forming radical ideas (i.e., becoming an extremist or radical) or doing radical acts (e.g., performing violent acts or terrorist activity). There are other unknowns in the field of radicalization research, from definitional ambiguity to the lack of any straightforward causal models that can adequately explain the circumstances in which radicalization takes place, both online and offline (Marwick, Clancy, & Furl, 2022). As such, the phenomenon of radicalization is highly complex, and a significant number of theories have been put forward to explain its formation. For example, Sageman (2011), argued that radicalization is mainly a bottom-up process that occurs largely outside the influence of formal organizations, and that social networks are the most important factor in radicalization, overriding external input from radical organizations. Others see radicalization as a top-down process that is hierarchically orchestrated on the part of the radical organization (Hoffman, 2017). Wiktorowicz (2005) in turn, argued that identity formation[1] is central to radicalisation and that depending on the individual circumstances, radicalization usually happens gradually and cumulatively.

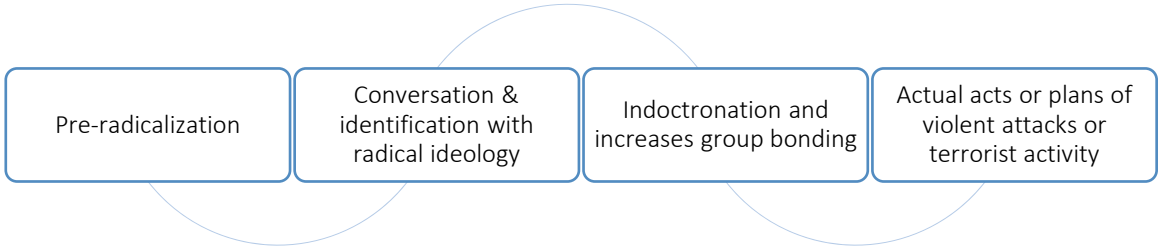
Koehler (2014) summarizes the theories of the radicalization process in four major schools: sociological, social movement, empirical and psychological theories. According to the sociological school, individuals claim a loss of identity in a hostile environment, which is the primary cause of radicalization. Briefly, the social movement theory argues that radicalization occurs due to the networks, group dynamics and peer pressure. The empirical school claims that individual's motivation for radicalization is to be found at the individual-level and according to socio-economic profiles. The psychological school contends that individual characteristics such as the emotional vulnerability, dissatisfaction with current political

[1] Identity formation refers to the process on how individuals explore and define their identity. It studies the differences in how individuals process identity relevant information and how they approach or evade the task of forming a sense of self-identity (Berzonsky, Cieciuch, Duriez, & Soenens 2011).

activity, identification with victims, belief that the use of violence is not immoral, a sense of reward and social ties into the radical group, are all important motivation for radicalization.

As different theories have been put forward, also various definitions exist to try to explain the singularities of radicalization. It does not surprise then that scholars have disagreed in the definitions of radicalization, and several exist in the literature. For example, Bittner (1963, p.929) argued that radicalism refers to *"a distinct philosophy and program of social change looking toward systematic destruction of what is hated, and its replacement by an art, a faith, a science or a society logically demonstrated as true and good and beautiful and just (…)."* Following this line of thought, a central characteristic of radical groups is that they consider their own group's norms or values as superior to those of other groups, which stablishes a 'us' against 'them' separation, which might serve as the basis for the use of violence. Precht (2007) summarized the concept of radicalization as *"(…) individuals who are frustrated with their lives, society or the foreign policy of their governments. A typical pattern is that these individuals meet other like-minded people, and together they go through a series of events and phases that ultimately can result in terrorism. However, only a few end up becoming terrorists. The rest stop or drop out of the radicalisation process at different phases."* Referring specifically to Islam radicalization, he argued a for four-step process of radicalization: pre-radicalization, conversation and identification with a radical ideology, indoctrination and increase group bonding and lastly, the actual violent activity (see Figure 1).

Figure 1: Precht's model of a radicalization pattern



Maskaliūnaitė (2015), in turn, defines the violent form of radicalization as a process by which an individual adopts a belief system that justifies the use of violence to effect social change and comes to actively support, as well as to employ, violent means for political purposes. For this research, however, we use McCauley and Moskalenko (2010) definition, that argues that radicalization is a change in beliefs, and behaviours in directions that increasingly justify intergroup violence and demand sacrifice in defence of the group. However, they note that this radicalization can manifest itself in both nonviolent and violent actions. In short, radicalization is as the set of processes by which one comes to engage in radical belief of any form, whether online or otherwise. However, the literature has found evidence that the internet facilitates most types of radicalization mechanisms (Baaken, & Schlegel, 2017).

Radical groups have different motivations and objectives for, Table 1 provides some examples.

Table 1: Different types of radical groups and their main objective.

Type	Main objective
Nationalistic or Separatist Groups	Obtain and secure a territory for the own group.
Extreme Right-Wing Groups	To safeguard the importance of the 'white race' that is perceived to be threatened by immigrants and other minority groups.
Extreme Left-Wing Groups	To achieve a just distribution of wealth and perceive capitalism as the primary problem.
Single Issue Groups	Their main concern focuses on one topic such as the environment or animal rights.
Religiously motivated Groups	They adhere to a very rigorous interpretation of their religion to justify violent activity against others.

Source: own elaboration adapted from Doosje, Moghaddam, Kruglanski, De Wolf, Mann, & Feddes, (2016).

Recent research on radicalization has debunked several myths associated with it. For example, there is no specific type of person that is vulnerable to radicalization, and most people who commit political violence are not mentally ill or alienated from society. Further, radicalization is not only caused by poverty, oppression, or marginalization, and viewing extremist media does not necessarily lead to adopting extremist beliefs or committing political violence. Moreover, self-radicalisation is rare, even for self-starters who radicalise on the internet there is a need for social interactions (Muro, 2016). Additionally, it appears that radicalization is gradual process that individuals go through, and not a rapid process as people often believe (Schmid, 2013). Individuals progressively embrace the common identities, feelings, and interpretations of a specific community and rationalize their problems as wrongs caused by others to justify using radical political attitudes or violence against them (Marwick, Clancy, & Furl, 2022). The literature argues that three overlapping, but distinct elements motivate individuals to becoming radicalized 1) the ideas of the radical narrative that provide a filter for understanding the world, 2) the sociological factors that compel an individual to embrace this radical narrative; and 3) the psychological factors and characteristics that may prompt an individual to use violence in order to promote or consummate this narrative (Borum, 2011).

Two clarifications must point out before continuing. First, a group or individual can hold radical views without necessarily taking radical actions (i.e., violent acts or terrorist attacks) (Neumann, 2013). Second, radicalization should not be confused with recruitment because it refers to what precedes an individual actually joining a radical or extremist organization

(Winter, Neumann, Meleagrou-Hitchens, Ranstorp, Vidino, & Fürst, 2020). The following section explores the ways of how radical groups use the internet to radicalize individuals.

3. Ways that Radical Groups Use Online Tools to Radicalize Individuals

In itself, the internet does not cause radicalization, however it can help spread radical ideas, enables people interested in radical beliefs to form communities, increases the international reach of those ideas, helps recruit individuals, enables the production and publication of propaganda, and may be used to spread distrust towards public institutions and the status quo (Weimann, 2004; Conway, 2005; Kimmage, 2008; Zelin, 2013). Recent studies have shown that internet tools are linked to violence and terrorist acts, for example, Gill et al. (2017) examined the role of the internet in terrorist activity within a sample of 223 convicted UK terrorists and concluded that the internet is a facilitative tool that allows for greater opportunities for violent radicalization and attack planning.

According to King and Taylor (2011), the internet facilitates the radicalization process through three different functions: ideological support, networking, and educational materials. In turn, Bastug, Douai, and Akca (2020) argue that social media networking platforms play a significant role in online radicalization in a four-step process: (1) accessibility/availability of extremist messages (i.e., online religious content), (2) susceptibility and individual's pre-disposition (i.e., social and psychological background of individuals/users), (3) terrorist mobilization (i.e., taking action), and (4) sharing/propagating (messaging and feedback loop). Additionally, most internet users might not be aware that they are consuming propaganda or other deceptive materials designed to radicalize or enlist followers.

A systematic review found tentative evidence that exposure to radical violent online material is associated with extremist online and offline attitudes, as well as the risk of committing political violence among white supremacist, neo-Nazi, and radical Islamist groups. Moreover, active seekers of violent radical material also seem to be at a higher risk of engaging in political violence as compared to passive seekers (Hassan et al., 2018). A study of radicalization of the NYPD Intelligence Division claimed to have identified the internet as a driver and enabler for the process of radicalization (Silber & Bhatt, 2007). A more recent study argued that internet accelerates individual radicalization processes through several pathways that include, more opportunities to become radicalised, providing an 'echo chamber' and increasing opportunities for self-radicalisation (Von Behr, Reding, Edwards, & Gribbon, 2013).

Another study carried out to German former right-wing extremist, found that the internet is a major driving factor to establish and foster the development of radical contrasting societies, transmitting radical and violent ideologies and translating them into political activism (Koehler, 2014). Other research found that online under-ground communities have contributed to the growth and propagation of the alt-right and other extreme right-wing ideologies (Hine et al., 2017; Zannettou et al., 2017). However, a report stated that specifically

for the youth, there is to date no empirical evidence to link radical groups use of internet and social media to actual violent radicalization (Alava, Frau-Meigs, & Hassan, 2017).

Authors have argued that radicals use of online tools can be separated in two main groups (Conway, 2005; Weimann, 2006). The first is classified as 'instrumental uses' and refers to the use online tools for planning, logistics and reconnaissance (e.g., search for addresses and book flights online), fundraising, disseminating training manuals and videos (e.g., on how to make bombs or procure weapons) and networking. The other classification refers to communicative uses, such as the use of technology for publicity and propaganda, generate political support, call the attention of the media, and recruit new followers. Nonetheless, it is important to note that there is little empirical knowledge about the actual process in which individuals become radicalized through online interactions and materials (Bastug, Douai, & Akca, 2020).

A significant amount of the literature, however, argues that in reality, the distinction between the offline and online radicalization processes is inconvenient. Scholars have reasoned that online radicalization is a contradiction and not representative of reality. Moreover, it creates a 'false dichotomy' which separates online processes of radicalization with those that take place offline (Hoskins & O'Loughlin 2009; Gill et al. 2017). In this sense, rather than being initiators or causes of violent behaviours, the online world is considered more a facilitator of radicalization.

4. Best Practices and Strategies to Counteract Online Radicalisation

The process of online radicalization is and multi-faceted phenomenon in which the internet through tools like social media, is used as a strategic instrument to try to incite radical behaviour. Neuman (2013) framed the measures to reduce prevent and counter radicalization in the following way, first efforts aimed at *reducing the supply* of all radical material, second, measures that seek to *reduce the demand* for radical messages and third, *exploiting online* content and interactions for the purpose of gathering information, gaining intelligence, and pursuing investigations. In turn, measures can be divided into analyses of defensive (or reactive) and offensive (or proactive). Several countries, most notably the US and the UK, have established specialized divisions to manage strategic communications initiatives in the context of combating radicalization and violent extremism online (Briggs, & Feve, 2013). This section presents the main tools and strategies to counteract online radicalization.

4.1. Reducing the Demand for Radical Content

One of the primary methods for stopping radicalization on social media and the internet is to combat online radical ideas directly or indirectly. Various authors have established that one of the most effective ways to decrease the capabilities of online radical groups is by reducing the actual demand for radicalization messages. This can be accomplished by discrediting, countering, and confronting online extremist narratives.

Pro-active strategies tend to take two major forms: online counter-narratives and grassroots anti-propaganda initiatives. The phrase "counter-narrative" has evolved to refer to a broad variety of operations with various goals and strategies, including public diplomacy, and focused initiatives to refute the beliefs of violent radicals and extremists. A central point of these strategies is that the content of a counter-narrative needs to be attractive and provide the right information that prevents individuals from being allured to a radical group. Zeiger and Gyte (2020) argue that this can be accomplished in three main ways, first, by deconstructing extremist arguments (pointing out the weakness in their logic), second, by undermining the credibility of the whole group, and lastly, by providing alternative narratives that emphasize a different course of action. Briggs and Feve (2013, p.16) argue that: *"Counter-narratives cover a broad range of strategies with different aims and messages, including picking apart violent extremist ideologies through eroding their intellectual framework; attempting to mock, ridicule, or undermine the credibility/legitimacy of violent extremist messengers; highlighting how extremist activities negatively impact on the constituencies they claim to represent; demonstrating how the means they adopt are inconsistent with their own beliefs; or questioning their overall effectiveness in achieving their stated goals."*

Importantly, these types of strategies should consider specific target audience through the local context of where these individuals are inhabiting, since credibility appears to be essential for counter-strategic communication campaigns (Winter, Neumann, Meleagrou-Hitchens, Ranstorp, Vidino, & Fürst, 2020). For example, the US based Carter Center published detailed reports focusing on how the Islamic State can be challenged through theological argumentation (Carter Center, 2016). In another example, in 2011, a partnership between London's Institute for Strategic Dialogue, Google Ideas and the Gen Next Foundation founded Against Violent Extremism (AVE). AVE is a global network of former extremists, survivors of violence and interested individuals from the public and private sectors that work together to counter all forms of extremism. This network is predominantly a counter-narrative project, and its main objective is to amplify the voices of former extremists and survivors as an effective way to counter radicalisation (Briggs & Feve, 2013).

Strategies can focus on promoting positive and alternative messages of radical groups, what is known as counter messaging. The goal of counter messaging is to spread ideas that are intended to undermine the attractiveness of radical messages by, for example, building positive identities and enhancing social cohesion. These types of messages usually take two forms, on the one hand they can ridicule or undermine the credibility of radical messages, on the other, they can provide positive alternatives that cancel out the radical ideology. Further, alternative narratives can offer a non-violent alternative that addresses community problems, and the underlying causes of radicalization. Websites, blogs, videos, and other forms of online social media can all be used to spread these messages. Nevertheless, the most immediate way to confront radical online propaganda directly is to go to the virtual forums and engage

actual and potential radical discussion, resting on the assumption that these ideas are based on falsehoods and conspiracy theories (Neuman, 2013).

These strategies, although impactful, tend to be limited in scope and in many instances, suffer from lack of funding. This policy weakness prevents them from maintaining their online presence and reaching out to a larger audience and have a bigger impact (Alava, Frau-Meigs, & Hassan, 2017). Moreover, as is often the case with security policies, lack of resources limits the capacity to evaluate the effectives of such programs and to adapt them to new challenges, as an ongoing process (Croci, Laycock & Chainey, 2022).

Another well knows strategy is to build capacity by equipping groups with the skills and knowledge to craft appealing messages and disseminate it among the people who are susceptible to online radicalization. The government must educate parents, teacher, and community leaders on the dangers of internet radicalization so that they can recognize, report, and act when it occurs. The formal education sector plays an important role in ensuring that individuals can differentiate between various kinds of strategies that are used by radical groups to spread their messages. As such, strengthening the overall education sector responses to radicalization, particularly violent activities, is crucial. In some countries, like France and the UK, as a preventive method, teachers and other educators are being trained to recognize early signs of online radicalization among their students (Alava, Frau-Meigs, & Hassan, 2017). In the United States, the National Counterterrorism Center (NCTC)[2] has developed awareness briefings that are used in roundtables and town-hall meetings with local communities (Neuman, 2013). Further, the private sector, particularly social media, and technology companies, can dedicated resources to educating the public on digital and media literacy skills. Relatedly, internet service providers should give enough funds to managing chat rooms and online forums, and they should update parental-filtering software to include websites that openly support extremism. As such, public-private cooperation and an inclusive approach is important in contributing to the enhancement of prevention efforts.

Centrally, however, the most long-term strategy to reduce the demand for online radical propaganda is to improve and promote media literacy, particularly among the youths. Governments should provide and support national and local level training programs that teach people how to use and how to promote media literacy and build capacity among communities. For example, it is central to teach internet users how to recognize the warning indications that virtual information is manipulative, deceptive, or misleading. Governments have backed a variety of projects where civil society organizations receive social media and communications training. For this purpose, a range of digital literacy tools have been developed, albeit being still scarce (Williams, Evans, Ryan, Mueller, & Downing, 2021). These tools may include courses that teach young people how to use the media critically, that help assess and challenge the sources of those contents, and that teaches how to separate

[2] For more information, see: https://www.dni.gov/index.php/nctc-home

unreliable information from information that is credible and trustworthy. Another example is to include information about the consequences of getting involved in radical groups and activities.

Increased activities and cooperation with civil society organizations, relevant local communities and non-governmental actors are important steps to reduce de demand of radical content. It is wise that governments acknowledge their role in contributing to the effectiveness of the implementation anti radicalizing plans and strategies since in many circumstances, they understand better the local dynamics. For example, the Radicalisation Awareness Network Policy Support[3]launched in 2021, is an EU-wide umbrella network connecting practitioners and field experts, that include social and health workers, teachers, prison staff, civil society organisations, victims' groups, representatives from local authorities, law enforcement, counter terrorism specialists and academics. These experts exchange ideas, experiences, identify good practices and issue recommendations on how to best tackle all forms of radicalisation, whether it is online or offline.

Another layer of the analysis is to use online content and interactions for the purpose of gathering information, gaining intelligence, and pursuing investigations. Researchers have argued that governments should take this strategy more seriously and use the internet to obtain intelligence, as it can be one of the best methods to combat online radicalisation, especially in the short term. Social network analysis[4] is a particularly useful tool to reach these objectives, since it can help understand who is part of what network, and how individuals interact with each other.

4.2. Reducing the Supply of Radical Content

One of the main methods used to avoid radicalization on social media and the internet is to employ technological tools and techniques to remove, filter and forbid the dissemination of radical or extremist information and propaganda. The logic is that the internet must not go beyond the law, as such, whatever domestic laws applies to other tools of communications (e.g., newspapers and radio) should also be enforced in the cyberspace. These tools might include legislative and policy actions, filtering, screening, and removing extremist information, and blocking content and access to social media platforms. Further, governments have placed heavy demands on private corporations to actively undermine the extremist networks that are present on their platforms, mostly by suspending accounts and censoring material (Fioretti, 2017).

Other tools include legislative measures and laws that set regulations for prosecuting individuals and organizations. For example, in Germany, there are penalties for organizations

[3] For more information, see: https://home-affairs.ec.europa.eu/networks/ran-policy-support_en

[4] Social network analysis seeks to understand networks and their members. The tool has two main focuses: the actors and the relationships between them in a specific social context.

that spread hate speech and fake news online that go up to 5 million euros for individuals and 50 million euros. Further, these organizations must take down posts containing hate speech or other criminal material within 24 hours of being identified (Miller, 2017). In another example, the European Parliament passed legislation called "Tackling the dissemination of terrorist content online"[5] in 2019 that focused on social media platforms content regulation and takedown. Based on this regulation, terrorist and radical content must be taken down within one hour after it is identified online and applies for online platforms offering services in the EU. It is important to note, that legislative approaches to tackle only radicalization face several difficulties. Since most politicians are not technology experts, there can occasionally be a misperception about how the internet and social media firms operate and what new technologies are available (Zeiger & Gyte, 2020). Centrally, the main flaw in these methods is that they only apply to locally hosted or run websites; no government has the authority to take down websites that are in other countries. Additionally, because only a small portion of radical information and discourse is actually illegal, it is frequently exempt from removal under the terms and conditions of the private sector.

Governments have also directly blocked social media channels and platforms of extremist groups or groups that foment radicalisation. These policies range from blocking individual websites and social media pages to blocking entire social media platforms. Another way to prevent the spread of radical content is through the takedown of individual posts or websites by technology companies themselves or by third parties. For example, the British Government established the Counterterrorism Internet Referral Unit (CTIRU) that is ran by the Metropolitan Police and responds to tips from the public, the police, and the intelligence agencies. CTIRU is staffed by a team of experts and employees of the Crown Prosecution Service that investigate websites that are suspected of breaking the law, in particular assess those that breach UK terrorism legislation[6]. By 2019 the organizations had secured the removal of over 310,000 pieces of terrorist material. Other strategies to eliminating the supply side include using cyberattacks to take down websites, bringing prosecutions against the owners or founders of the website and cooperating with private sector platforms to take down or hide (by making it more difficult for people to find radical content through the manipulation of search results or the removal of suggested links or webpages) radical content (Neuman, 2013).

However, these types of strategies are considered as a short-term solution, since radicalised groups can rapidly use new platforms and channels of communications. Further, there are

[5] For more information see: "Tackling the dissemination of terrorist content online European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019AP0421

[6] The Terrorism Act (2000) is the primary piece of counter-terrorism legislation in the UK. Other relevant legislation includes: the Anti-Terrorism, Crime and Security Act (2001), Terrorism Act (2006) and the Counter Terrorism Act (2008).

important limitations on the effectiveness of this response, given the speed with which new information is uploaded or changed and the limited capacity of law enforcement agencies (Briggs & Feve, 2013). Importantly, it has been argued that blocking access or the publishing of content in social media is an infringement of fundamental human rights. Moreover, this is a risky path for governments to take since parameters of what is acceptable and what is not, may change depending on political affiliation or the government in turn. For example, blocking content has been used to prevent the spread of ideas of political opposition groups (Zeiger & Gyte, 2020).

As a final point, the literature shows that attempts to reduce the supply dimensions of online radicalization does not have proven efficacy. For example, in a recent report from UNESCO (2017), concluded that there is to date no empirical evidence to suggest that social media (e.g., Facebook or Twitter) self-regulatory measures help reduce violent radicalization outcomes among young people, nor is there any evidence to contradict this possibility. Further, these types of strategies tend to conflict with the essential task of gaining intelligence that can be useful to pursue radical groups and prevent possible acts of violence (Neuman, 2013). Importantly, reducing the supply of extremist content on the internet is costly and may be counterproductive as the strategy can have damaging effects, particularly regarding freedom of expression, freedom of information, privacy, and the right to association (Alava, Frau-Meigs, & Hassan, 2017). As such, these types of strategies should be used as a last resort and with specific short-term objectives.

5. Conclusions

Radicalization is used to refer to the process of developing extremist ideologies and beliefs that increasingly justifies violence against other groups or symbolic targets, in an effort to alter their behaviour and forward the radical group political ambitions. However, high level of radicalization does not necessarily equal a high level of violent behaviour, or any physical violent behaviour at all. Scholars tend to agree that radicalization is a gradual process that usually happens with a combination of online and offline practices. Policymakers still frequently attempt to neatly divide the online and offline spheres, but scholarly research has shown that such separation, in most cases, cannot be made. The fact is that it is not the most effective strategy to combat radicalism online, without also attempting to comprehend and confront its offline manifestations. As such, there is a need to further explore and research how both online and off-line platforms intertwine and harnessed individuals towards radicalization.

During the last decades, radical groups have used internet tools and social media, to attract and recruit individuals to their cause. Radical groups have become particularly adept at utilizing new media, and they are making effective use of the internet and social media as delivery and distribution channels of propaganda. Radical propaganda not only aims to radicalise the vulnerable, but to inspire those further along the radical path into violent

activities. The internet through message forums, social networking sites, streaming services, static websites, and encrypted communication tools allow radical organizations to coordinate actions, disseminate propaganda, recruit new members, and exchange training materials, among other things. Although many websites try to prevent or remove white supremacist and other extremist information from being published on their sites, inconsistent enforcement practices and the availability of more lenient alternative technological websites allow these movements to continue openly coordinating online.

As a first step to decrease the influence of radical groups, the government should take a more active role in lowering the demand for radical online content, for instance, by encouraging youth awareness and education. Governments should also develop a plan for strategic communications that addresses the issue of fending off radical propaganda on the internet and social media. A comprehensive strategy to counter radicalisation needs to consider the individual, organisational and societal level on how individuals become radicalized. Further, they should also think about establishing centralized offices to manage and organize this strategy. In addition to increasing public awareness of the threat posed by radicalism, government actions must make sure that its positions and policies are clearly stated and targeted at the appropriate audiences and contexts. As this report has shown, the credibility of government actions is central for counter-strategic communication campaigns. In this sense, government strategies will be particularly impactful if they also focus on forging relationships with specific communities that can directly challenge false information. As a final point, public institutions should stablish and deepen its partnership and cooperation with the private sector. In many cases, these companies are in a strategic position to combat online radicalism, particularly in such a fast changing and evolving environment as the internet.

References

Alava, S., Frau-Meigs, D., & Hassan, G. (2017). Youth and violent extremism on social media: mapping the research. UNESCO Publishing.

Baaken, T., & Schlegel, L. (2017). Fishermen or swarm dynamics? Should we understand jihadist online-radicalization as a top-down or bottom-up process?. Journal for Deradicalization, (13), 178-212.

Bastug, M. F., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. Studies in Conflict & Terrorism, 43(7), 616-637.

Berzonsky, M. D., Cieciuch, J., Duriez, B., & Soenens, B. (2011). The how and what of identity formation: Associations between identity styles and value orientations. Personality and Individual differences, 50(2), 295-299.

Bittner, E. (1963). Radicalism and the organization of radical movements. American Sociological Review, 928-940.

Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. Journal of strategic security, 4(4), 7-36.

Bötticher, A. (2017). Towards academic consensus definitions of radicalism and extremism. Perspectives on terrorism, 11(4), 73-77.

Briggs, R., & Feve, S. (2013). Review of programs to counter narratives of violent extremism

Conway, M. (2012). From al-Zarqawi to al-Awlaki: The emergence of the Internet as a new form of violent radical milieu. Combating Terrorism Exchange, 2(4), 12-22.

Correa, D., & Sureka, A. (2013). Solutions to detect and analyze online radicalization: a survey. arXiv preprint arXiv:1301.4916.

Croci, G., Laycock, G., & Chainey, S. (2023). A realistic approach to policy formulation: the adapted EMMIE framework. Policy Studies, 44(4), 433-453.

Doosje, B., Moghaddam, F. M., Kruglanski, A. W., De Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. Current Opinion in Psychology, 11, 79-84.

Fioretti, Julia. 2017. Social Media Giants Step Up to Join Fight Against Extremist Content. Reuters, 26 June. https://www.reuters.com/article/us-internet-extremism/social-media-giants-step-up-joint-fight-against-extrem-ist-content-idUSKBN19H20A.

Frissen, T. (2021). Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults. Computers in Human Behavior, 114, 106549.

Galland, O., & Muxel, A. (2020). Radicalism in Question. In Radical Thought among the Young: A Survey of French Lycée Students (pp. 1-23). Brill.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. Criminology & Public Policy, 16(1), 99-117.

Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., ... & Sieckelinck, S. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. International journal of developmental science, 12(1-2), 71-88.

Hine, G., Onaolapo, J., De Cristofaro, E., Kourtellis, N., Leontiadis, I., Samaras, R., ... & Blackburn, J. (2017, May). Kek, cucks, and god emperor trump: A measurement study of 4chan's politically incorrect forum and its effects on the web. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 11, No. 1, pp. 92-101).

Hoffman, B. (1998). Inside Terrorism New York. NY: Columbia University Press [Google Scholar].

Kimmage, D. (2010). Al-Qaeda central and the internet. March, Washington DC: New America Foundation.

King, M., & Taylor, D. M. (2011). The radicalization of homegrown jihadists: A review of theoretical models and social psychological evidence. Terrorism and political violence, 23(4), 602-622.

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the Internet. Journal for Deradicalization, (1), 116-134.

Marwick, A., Clancy, B., & Furl, K. (2022). Far-Right online radicalization: A review of the literature. The Bulletin of Technology & Public Life.

Marwick, A., Clancy, B., & Furl, K. (2022). Far-Right online radicalization: A review of the literature. The Bulletin of Technology & Public Life.

Maskaliūnaitė, A. (2015). Exploring the theories of radicalization. International Studies: Interdisciplinary Political and Cultural Journal (IS), 17(1), 9-26.

McCauley, C., & Moskalenko, S. (2010). Recent US thinking about terrorism and counterterrorism: Baby steps towards a dynamic view of asymmetric conflict. Terrorism and Political Violence, 22(4), 641-657.

Miller, J. (2017). Germany votes for 50m euro social media fines. British Broadcasting Corporation News.

Muro, D. (2016). What Does Radicalisation Look Like? Four visualisations of socialisation into violent extremism. Notes internacionals CIDOB, 163, 1-5.

Neumann, P. R. (2013). Options and strategies for countering online radicalization in the United States. Studies in Conflict & Terrorism, 36(6), 431-459.

Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. Terrorism and Political Violence, 28(1), 1-29.

Precht, T. (2007). Home grown terrorism and Islamist radicalisation in Europe. Retrieved on, 11.

Sageman, M. (2011). Leaderless jihad: Terror networks in the twenty-first century. University of Pennsylvania Press.

Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT research paper, 97(1), 22.

Schuurman, B., & Taylor, M. (2018). Reconsidering radicalization: Fanaticism and the link between ideas and violence. Perspectives on Terrorism, 12(1), 3-22.

Sedgwick, M. (2010). The concept of radicalization as a source of confusion. Terrorism and political violence, 22(4), 479-494.

Silber, M. D., Bhatt, A., & Analysts, S. I. (2007). Radicalization in the West: The homegrown threat (pp. 1-90). New York: Police Department.

Von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the digital era. The use of the internet in, 15.

Weimann, G. (2004). www. terror. net: how modern terrorism uses the Internet (Vol. 31). United States Institute of Peace.

Weimann, G. (2006). Terror on the Internet: The new arena, the new challenges. US Institute of Peace Press.

Whittaker, J. (2022). Rethinking online radicalization. Perspectives on Terrorism, 16(4), 27-40.

Wiktorowicz, Q. (2005). Radical Islam rising: Muslim extremism in the West. Rowman & Littlefield Publishers.

Williams, H. J., Evans, A. T., Ryan, J., Mueller, E. E., & Downing, B. (2021). The Online Extremist Ecosystem: Its Evolution and a Framework for Separating Extreme from Mainstream. RAND.

Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: research trends in internet activism, radicalization, and counter-strategies. International Journal of Conflict and Violence (IJCV), 14, 1-20.

Zannettou, S., Caulfield, T., De Cristofaro, E., Kourtelris, N., Leontiadis, I., Sirivianos, M., ... & Blackburn, J. (2017, November). The web centipede: understanding how web communities influence each other through the lens of mainstream and alternative news sources. In Proceedings of the 2017 internet measurement conference (pp. 405-417).

Zeiger, S., & Gyte, J. (2020). Prevention of Radicalization on Social Media and the Internet. International Centre for Counter-Terrorism (ICCT).

Zelin, A. Y. (2013). Libya Beyond Benghazi. Journal of International Security Affairs, (25).