PREPARED BY *Passalacqua Matteo (from Belgium)*

Mail : m.passalacqua@hotmail.be

ONLINE RADICALISATION & CYBERSECURITY

CASE STUDY : BELGIUM

PREPARED FOR

Cybersecurity & cyberwarface courses

2024

University of Bologna

Online radicalisation is now a major challenge for national and international security, in an increasingly connected and technology-dependent world. With the advent of the Internet and social networks, the spread of extremist discourse and the radicalization of certain populations have reached alarming proportions, posing complex and multifaceted challenges to social and political stability. In this context, Belgium, as a European country that is very connected to social diversity, is no exception to this worrying reality.

In a world where digital communication is ubiquitous, online platforms have played a central role in the spread of radicalisation and extremism. Social media, online forums, and instant messaging platforms have become preferred vehicles for the dissemination of extremist propaganda, making it easy for radical groups to reach a global audience. (Courbet et al., 2015) The speed and scale of this spread have contributed to the proliferation of the problem, with individuals being exposed to radical content without even realizing it, thus increasing the risks of radicalization. Indeed, more and more researchers and NGOs see the digital environment as a means of radicalization, describing it as a kind of "terrorist incubator".

Belgium, as a European nation at the heart of the continent, is particularly vulnerable to these challenges. Its culturally, ethnically and religiously diverse population creates fertile ground for the exploitation of marginalized communities, who may feel alienated and seek refuge in extremist ideologies, especially online. The tragic terrorist incidents that have occurred in Belgium and other European countries have underlined the urgency of understanding and countering online radicalisation, highlighting the need for swift and coordinated action. (Dumoulin, 2021). It is therefore questionable what are the individual, social and technological factors that contribute to online radicalisation, how these specific dynamics influence national as well as international security and social cohesion in a context of cultural and religious diversity, and what cybersecurity strategies can be deployed to counter this growing threat and ensure the safety of European citizens.

Therefore, this work aims to explore in depth the multiple facets of online radicalisation and its implications, as well as the dynamics of online radicalisation, highlighting the specific challenges that Belgium, but more specifically Europe, faces in this crucial area for security and social cohesion. To do this, we will start by understanding the context and the theoretical framework, which are essential elements for analysing the whole of online radicalisation. Then, we will examine the underlying dynamics of this phenomenon, highlighting the individual, social, and technological factors that contribute to the radicalization of individuals. In addition, we will analyse the role of social networks in the process of online radicalisation, and try to find out whether the European Union and the various online platforms are taking measures to counter this phenomenon. Finally, we will look at whether it is really possible to prevent radicalisation and propose possible ways to counter radicalisation online. In addition, we will also analyse the cybersecurity strategies deployed by the Belgian authorities to counter this growing threat and ensure the safety of its citizens. Although Belgium has taken a proactive approach to countering online radicalisation, the implementation of legislative measures, public-private partnerships and awareness programmes to counter this threat. However, despite these efforts, persistent challenges remain, including coordination between different actors, protecting citizens' privacy and adapting to new technologies. At the end of this work, a brief conclusion can be drawn.

This work will provide an in-depth analysis of the European challenges in terms of online radicalisation and propose possible recommendations to strengthen Belgium's, but more specifically Europe's, response to online radicalisation, in order to be able to improve the security and stability of the old continent in an ever-changing digital world.

Context

Online radicalization and cybersecurity are intrinsically linked, forming a crucial issue for national and international security. This connection stems from how extremist activities on the internet pose a pervasive threat, exploiting digital flaws to spread their violent ideologies and recruit new followers. In this complex landscape, a thorough understanding of the global context becomes imperative to develop effective strategies to prevent and counter online radicalisation.

The internet acts as a catalyst, providing individuals with an unprecedented platform to explore and express alternative identities. This freedom of expression often resonates with fringe affiliations and stigmatized beliefs, where individuals can connect with others who share similar interests, creating online ecosystems conducive to radicalization. (Lauw et al., 2010) This phenomenon is exacerbated by the ability of social networks to facilitate interactions between strangers with deviant beliefs, a dynamic that was once constrained by geographical and social barriers.

Technological advances have also upset the balance of power in the communications landscape, allowing extremist groups to circumvent traditional state-imposed barriers. New information and communication technologies (ICTs) have broken the asymmetrical dynamics of traditional

conflicts, providing terrorists with effective ways to spread their message and recruit new members. Physical borders can no longer guarantee the isolation of terrorist groups, as their influence extends beyond geographical boundaries through a permanent virtual presence on the Internet. (McKenna, 2007)
The strategic use of the Internet by terrorist groups goes beyond the mere dissemination of propaganda. ICTs have become tactical tools of psychological warfare, harnessing the power of the media to instill terror and manipulate perceptions. (Weimann, 2005) Striking examples are the dissemination of offensive images to promote terrorist narratives and the creation of sophisticated websites adopting marketing techniques to attract new sympathizers. This skillful use of ICTs underscores the need for innovative approaches to counter online radicalisation.

In this context, it is also crucial to understand the theoretical underpinnings behind these efforts. A thorough understanding of theories of terrorism, radicalization, individual and social psychology, as well as mechanisms of online manipulation is essential to design effective initiatives. The next point will address these theoretical bases in detail to better understand strategies to counter online radicalisation in the future.

Theoretical framework

Terrorism, as a complex and often debated phenomenon, requires an in-depth analysis of its causes and dynamics, especially in the context of online radicalisation. Understanding the origins of terrorism and the radicalization processes that lead to it is essential to develop effective prevention and intervention strategies.

Theories about the causes of terrorism, as Jeff Goodwin points out, vary according to the very definition of terrorism. (Goodwin, 2006) Moreover, Friedland evokes terrorism both as a form of violent resistance to the state and as a tool in the service of the state's interests. (Friedland, 1988) Goodwin adds to this definition by describing it as the targeting of civilians or non-combatants to intimidate others. But why do states or non-state groups resort to this violence? This question underscores the importance of knowing whether civilians are supporters of the state or rebels to understand whether they will be attacked by terrorist acts.

Prior to September 11, 2001, two dominant assumptions about the causes of terrorism were preponderant: First, the theory of despair, where terrorism is perceived as the weapon of last resort of the weak, and retaliation against the violence of the enemy, usually the state; Second, the theory of radicalization, which posits that individuals engage in extremist beliefs

and behaviors due to different factors that push them down this path. This can include feelings of marginalization, frustration, or social injustice, as well as ideological or social influences that reinforce these perceptions. (Randall, 2019)
However, post-9/11, the theory of radicalization gained prominence, highlighting the link between radicalization and terrorism.

Toro Bjorgo and Andrew Silke criticized the analytical effectiveness of the "root causes" of terrorism, stressing the need to distinguish between explanations of prevalence and explanations of specific terrorist incidents. The preconditions and triggers of terrorism offer an in-depth perspective on the origins and dynamics of this complex phenomenon. Preconditions provide fertile ground for the emergence of terrorism, resulting from general and structural conditions within a society. Among these conditions, the absence of democracy, civil liberties and the rule of law creates an environment conducive to the rise of terrorism. Illegitimate and corrupt national authorities, often supported by foreign governments, fuel feelings of social injustice and ethnic or religious discrimination, thus reinforcing the motives for radicalization. In contrast, the triggering factors are specific incidents or situations that directly motivate the emergence of terrorism. These triggers can be observed at different levels. Macro factors encompass systemic conditions such as deep-rooted conflicts, invasion by foreign forces, economic underdevelopment, and widespread corruption. These factors provide a context conducive to the emergence of terrorism by exacerbating social and political tensions. (Bjorgo and Silke, 2018)
At an intermediate level, meso factors include the activities of terrorist organizations, social movements, and charismatic leaders who mobilize the masses. These group dynamics can amplify feelings of marginalization and injustice, leading to increased radicalization. Finally, micro-factors focus on individuals and interactions in small groups. Individual radicalization can be influenced by factors such as ideological indoctrination, personal experiences of discrimination or marginalization, and social interactions with radicalized peers. It is rather these micro-factors that affect Europe in terms of radicalisation. (Bjorgo and Silke, 2018)
Economic factors and civil liberties also play an important role in the genesis of terrorism. Although poverty is often seen as a root cause, its connection to terrorism is mixed. In contrast, state repression and human rights violations are stronger predictors of terrorism, highlighting the importance of political and social conditions in radicalization.

It is important to note that the boundaries between these levels are not clear, and developments at one level can have an impact on the other levels. For example, meso or micro events, such as the publication of controversial cartoons or information about international conflicts, can influence the perception and attitudes of individuals at the macro level.

By considering these key factors, such as economic conditions, human rights, political representation, and media effects, we can better understand the underlying mechanisms of radicalization and terrorism. This more nuanced understanding is essential for developing effective prevention and intervention strategies, considering both the structural causes and the specific triggers that fuel terrorist violence.

Radicalization

Radicalization, whether online or offline, and which has become a central topic since the tragic events of September 11, 2001, is a complex and multifactorial process that requires in-depth analysis to grasp its full scope. Since then, the concept of radicalization has gained prominence, especially after events like the Madrid and London attacks, becoming a key pillar in understanding what drives individuals to engage in terrorist acts.

First, to define radicalization, it is essential to recognize its relational and value-laden nature. Indeed, being considered "radicalized" depends largely on the social norm or central set of ideas of a given society at a given time. Thus, radicalization can be seen as a social and psychological process of progressive commitment to extremist political or religious ideologies. However, radicalization can also be conceptualized behaviorally or cognitively, depending on whether the focus is on accepting radical ideas or directly supporting terrorism. (Neumann, 2015) This diversity of definitions reflects the nuances and complexities of the phenomenon, influencing the construction of radicalization models and the policies that result from them.

Secondly, push factors play a crucial role in the radicalisation process. Perceptions of injustice, deprivation, and alienation are often catalysts, making individuals vulnerable to indoctrination and identification with groups sharing similar grievances. (Horgan, 2008) Experiences of discrimination, particularly in the context of counter-terrorism policies, can reinforce these feelings of exclusion and marginalization, thus nurturing the breeding ground for radicalization.

Socialization within radical groups provides a context for validating extremist beliefs and justifying violence as a means of defense and revenge. Progressive indoctrination and adherence to a dehumanizing ideology reinforce this justification, while consolidating

identification with the "ingroup" and the demonization of the "outgroup." (McCauley & Moskalenko, 2011)
Despite the potential risks and costs, there are powerful pull factors that encourage individuals to take the plunge into terrorism. The idea of being considered honorable, heroic, or martyred can exert significant influence, reinforced by the prospect of increased status within the group and community.

Finally, regarding online radicalization, these theories can be applied to a typology of radicalization specific to the internet, by highlighting different ways in which the Internet influences the evolution of beliefs towards extremes, including violence.
First, "pure online radicalized" represent those whose path to extremism originates and develops primarily through the internet and social media. These individuals are exposed to radicalizing narratives and narratives online, which gradually leads them to adopt increasingly extreme ideologies, sometimes to the point of justifying violence. This category of radicalization is characterized by the relative isolation of individuals, for whom the process often takes place autonomously, taking advantage of the anonymity offered by the digital world. Second, there are radicalization pathways where the Internet acts as an amplifier, reinforcing tendencies that were already present in individuals before they were immersed online. In this case, the Internet plays a crucial role in consolidating radical beliefs initiated offline, providing online content that reinforces these beliefs, or facilitating access to new digital social circles that encourage adherence to extremist ideas. Third, there are journeys where the Internet acts as a catalyst, gradually introducing individuals to radical ideas and milieus. While these individuals may initiate their radicalization online, they often then seek real-world interactions to share and reinforce their beliefs. The internet in this context plays a more informative role, providing answers and models for those who question their beliefs, but end up looking for more tangible interactions offline. (Horgan, 2017)

The causes of online radicalization

Online radicalization is a complex process influenced by a multitude of individual, social, and technological factors. Understanding these mechanisms and causes is crucial to developing effective prevention and intervention strategies.

First, easy access to the internet and social media has created an environment conducive to the spread of extremist propaganda. Online platforms provide a global reach for radical groups, allowing them to recruit new members and spread their ideologies on a large scale. (Courbet et al., 2015) The recommendation algorithms used by these platforms amplify this dissemination by recommending content like what the user has already viewed, thus creating filter bubbles that reinforce existing beliefs.

In addition, online radicalization is often the result of clever psychological manipulation by extremist groups. These groups exploit individuals' psychological vulnerabilities, such as feelings of isolation, a desire to belong, and a search for meaning, to attract them. By using sophisticated recruitment tactics, such as individual targeting and creating emotional narratives, they manage to radicalize certain individuals and inspire them to take action. (Blanchard, 2007) Indeed, Europe's cultural and religious diversity creates fertile ground for the exploitation of certain marginalized communities by extremist groups online. People who feel alienated or excluded from society are particularly vulnerable to manipulation and may take refuge in extremist ideologies that offer them a sense of belonging and camaraderie. Extremist groups exploit these feelings of marginalization and injustice to recruit new members and spread their ideology.

Finally, online radicalization is often a gradual process that takes place over a long period of time. Individuals can be exposed to extremist content for months or even years before taking action. (Pauwels et al., 2016) During this period, they may be progressively conditioned to engage in extremist beliefs and behaviors, making it difficult to detect radicalization early and prevent terrorist attacks.

By understanding the reasons for online radicalisation, it becomes clear that extremist groups use propaganda videos or images to convince and radicalise a wide audience. Indeed, it often happens that these "weaker" individuals allow themselves to be influenced by a single word (such as racial profiling, discrimination, migration, Palestine, unemployment, etc.) or by a single image. In these circumstances, people who are more psychologically vulnerable or less educated may be likely to continue their research on these topics. Subsequently, the algorithm present on social networks will offer these individuals a multitude of content related to their previous searches, which often includes radical or extremist content. (Horgan, 2008)

Extremists have grasped this strategy perfectly, developing videos and specific language to manipulate the emotions of a wider audience. This allows them to spread their messages through social media algorithms.

The role of social networks

Social networks play a crucial role in the construction of individual and collective identity. Studies reveal the existence of a process called "identity fusion" (Swann Jr et al., 2015), by which the individual gradually abandons his or her identity in favor of a radicalized group identity. This phenomenon is particularly pronounced among young people in search of social belonging, who may be seduced by the ideology of a terrorist group (Lindekilde et al., 2019).

First of all, this phenomenon of "identity fusion" is partly explained by the theory of "deindividuation" which underlines the rupture between individual and group identity fostered by the proliferation of virtual identities in the digital world. This deindividuation is fueled by the need for young people to forge new social connections through virtual meetings and online discussions, thus strengthening their sense of belonging to a virtual community. Interestingly, this sense of online presence often exceeds that of offline social interactions. (Reicher et al., 1995)

In addition, social networks, which play on the emotional and community character, exploit the vulnerability of young people through algorithms (Busher, 2015), positioning their membership as a potential step towards violent radicalization. However, more research is needed to conclusively establish a causal link in this area and to validate this claim.

In addition, social networks have undeniably revolutionized our interactions and our consumption of information. In the context of online radicalization, their role becomes crucial, serving as amplifiers of extremist ideologies. New social media have transformed communication by allowing for an instantaneous and global exchange of ideas. This speed and reach has been exploited by extremist individuals and groups to propagate their ideology and recruit new members. (Swann Jr et al., 2015) Platforms like Facebook, Twitter, and YouTube have become breeding grounds for attracting young people to radical causes, creating an unprecedented recruitment pool. In addition, these social media are formidable propaganda tools. Extremist content, in the form of videos, images and messages, is widely disseminated, saturating users' news feeds and contributing to the normalization of radical discourse within some online communities. In addition, online radicalization is facilitated by the easy access and relative security offered by these platforms, allowing individuals to connect anonymously with groups that share their beliefs, creating echo chambers where extreme ideas thrive and reinforce each other.

Finally, this repeated exposure to extremist content can influence the attitudes and behaviors of individuals, pushing them towards increasingly radical positions. (Riva et al., 2007) The normalization of extremism in online spaces creates an environment where marginal views become commonplace, exacerbating the phenomenon of social polarization. Social media has a significant impact on identity building, both on an individual and collective level.

A 2022 study of 17- and 18-year-olds in Switzerland by the Zurich University of Applied Sciences (ZHAW) and the Fribourg University of Social Work gives early indications of the impacts of social media on young people: First, when it comes to right-wing extremism, the results are worrying. Among young people with no immigrant background, about 6% were considered to belong to the far right. A quarter of these young people held xenophobic views, while 21% declared themselves nationalists. Even more worryingly, 3% of the young people interviewed had engaged in violent right-wing extremist behaviour in the year preceding the survey, and 5% were in favour of the use of violence against foreigners; Secondly, regarding left-wing extremism, the results show a significant presence of this trend among the young people interviewed. 7% of them were identified as being far left. Of these, 47% expressed anti-capitalist views, while 22% had a marked dislike of the police and the state. In addition, 8% said they were in favour of the use of violence against law enforcement, and around 4% had been involved in violent acts in the previous year; Finally, about Islamic extremism, although the percentages are relatively smaller, they are still significant. About 3% of young people from the Muslim faith were considered radical Islamists. Of these, 43 percent had a negative view of the West, and 29 percent disapproved of non-traditional Muslims. (ZHAW et al., 2022)
In short, these results can be interpreted for the whole of Europe and highlight the importance of understanding and addressing the different forms of extremism among young people in Europe, as it is these young people who will shape the world of tomorrow. In addition, this study highlights that this study represents only a small part of the population and therefore the need for proactive action to prevent radicalisation and promote values of tolerance, respect and mutual understanding.

In the face of this reality, governments and policymakers are increasingly concerned about preventing online radicalisation. They are actively looking for ways to counter the influence of new social media on people's attitudes and behaviours. However, empirical research on this complex relationship remains limited, highlighting the urgency of developing a deep understanding of this phenomenon to develop effective cybersecurity and prevention strategies for online extremism.

What is the European Union doing?

The fight against terrorism is primarily the responsibility of nation states, but since the Internet knows no borders, the EU is also trying to act against terrorists and extremists.

The European Union is deploying a range of strategies to try to effectively counter online radicalisation. Indeed, it works to strengthen legislation to sanction extremist content on digital platforms, while preserving fundamental rights such as freedom of expression. This legislative approach aims to establish common standards for the moderation of online content across EU Member States, creating a coherent regulatory framework to combat the spread of radicalisation on the internet. (European Council & Council of the European Union, 2024).

At the same time, the EU promotes international cooperation to counter online radicalisation. By collaborating with partners around the world, such as international agencies or online platforms, it facilitates the exchange of information and best practices in preventing and combating hate speech and online indoctrination. This cooperation not only allows for a better understanding of the dynamics of radicalisation, but also for the development of more effective and globally adapted strategies. However, this collaboration can often be hindered in the name of freedom of expression and human rights. (European Council & Council of the European Union, 2024).

Since 2015, in The Hague, Europol has been operating a European Counter-Terrorism Centre, a unit that identifies terrorist content online and then informs service providers such as Telegram or Google for its removal. Europol says it has eliminated around 5,000 accounts linked to the Islamic State terrorist group in recent years. (Arte, 2024).

Europol's intervention process seems rather simplistic, given that no specific legislation is in place in Europe to support this fight. Indeed, Europol agents only send recommendations to platforms to remove extremist accounts or content. However, the final decision rests with the platforms themselves, which means that there is no enforcement but rather implementation based on private contracts, in this case the general terms of use of the platforms (Facebook, Twitter, etc.).

In mid-2021, a European regulation allowing national authorities to order the removal of terrorist content came into force, and the platforms concerned must now react within the hour. Indeed, it is a "firewall" against terrorist content online to remove it from the web and prevent its dissemination (Official Journal of the European Union, 2021)

However, according to many MEPs as well as some NGOs working in favour of digital rights, this is not a major step forward as no member states have yet used it. Indeed, none of the tools introduced by this law since it was adopted, i.e. the powers conferred by this law on the competent authorities to combat extremist content, are used. No EU states use this European law. The reason for this non-use of European law is quite simple, because if an authority requires that content be removed within the next hour, it does not allow for adequate control to determine whether this content is extremist or not. In addition, cross-border removal orders are possible. For example, if an injunction comes from a country with an extremist or authoritarian government, such as Hungary, Poland, Italy, etc., the publication should be removed, even if it is perfectly legal in Belgium or Germany. (Grassegger, 2022).

There are serious problems with this legislation because, as I mentioned earlier, the definition of terrorism varies considerably from country to country, from institution to institution. For example, in Spain, terrorism also includes the independence movement, while in Hungary, migration is associated with terrorism. The question of the Middle East is also the subject of heated controversy throughout Europe.

Despite the European Union, which seems relatively paralyzed by this situation, one may wonder what the role of the different social media platforms in the fight against online radicalization is.

What do internet platforms do?

To fight against online radicalisation, the European Union and the Member States want to involve the internet giants, such as Facebook, X (formerly Twitter), YouTube, etc. Therefore, these different platforms must actively engage and swiftly remove hate messages or terrorist content. However, does it work?

In the case of Twitter, rather bad, because since Elon Musk bought the company in 2022, which he renamed "X", a large part of the moderation team has been fired. Since this takeover,

hate and fake news have increased massively. Elon Musk has chosen an extremely lax policy about the expression of hateful, dangerous, insulting and discriminatory content towards certain populations. As a result, users who want to express themselves in this way feel empowered to do so, knowing that they will not be censored. (Borelli, 2024).
In addition, new challenges are constantly emerging on the internet such as the rise of encrypted communication platforms, which offer extremists a safe space to spread their ideology without fear of detection. In response to this competition, major platforms such as Messenger and WhatsApp (Meta), Telegram, etc. offer the ability to further encrypt their conversations with the "enhanced chat security" feature. This increasing use of cryptography poses a major challenge for authorities responsible for monitoring and moderating online content, as it makes it more difficult to detect extremist and terrorist activities.

Facebook, Microsoft, X and YouTube have nevertheless created a forum to seek common technical solutions to fight terrorist content. The forum was built in 2015 in the wake of the terrorist attacks with the aim of bringing together the major platforms with considerable power over the flow of information online to governments. Thus, governments are trying to influence the content moderation policies of large platforms through this informal structure of public-private cooperation. (Weimann, 2010)
In addition, the global nature of the Internet makes coordination between different jurisdictions complexes. While tech companies operate globally, laws and regulations vary from country to country, which can lead to legal conflicts and obstacles to international cooperation in countering online radicalization. For example, content that is considered illegal in one country may be perfectly legal in another, making it difficult for internet platforms to determine what content should be removed.

Nevertheless, the task remains arduous and raises concerns about the real effectiveness of these measures. Indeed, although internet platforms strive to quickly remove terrorist and hateful content, it is difficult to guarantee full surveillance and perfectly effective moderation. Technical challenges, such as accurately identifying problematic content and setting up reliable automated moderation systems, persist. It is important to recognise that the fight against online radicalisation cannot rely solely on moderation and removal of content. (Borelli, 2024). Therefore, it is also essential to invest in awareness-raising and education initiatives to build the resilience of individuals against extremist propaganda and hate speech.
In addition, the question of freedom of expression also arises. While countering online radicalisation requires strong moderation measures, it is essential to strike a delicate balance

between removing extremist content and respecting users' freedom of expression. Internet platforms must therefore carefully navigate these competing imperatives, ensuring that fundamental rights are not compromised while addressing threats of radicalisation online.

Can radicalisation really be prevented online?

To effectively counter online radicalization and violent extremism, various strategies are proposed by counterterrorism experts. However, it is important to note that it is difficult, if not impossible, to completely prevent radicalization.

Radicalization can be influenced by many factors, including social, economic, and political elements, and often radicalized individuals are already engaged in extreme thought processes even before they are exposed to extremist ideologies online: First, it is recommended to focus on strategic counterterrorism communication. This involves monitoring and even rewriting the narratives propagated by terrorists in order to counteract their ideology. One approach is to hire community managers who specialize in counter-narratives, thus forming a form of virtual counterterrorism ; Second, an innovative approach suggests the commercialization of rival ideological products. For example, at the level of Islamist radicalization, it is crucial to identify dissenting opinion leaders to Islamism on online forums and convince them to spread counter-narratives advocating peaceful Islam. These messages must emanate from the Muslim community in a subtle way to increase their credibility, especially among young people; Third, it is imperative to develop more systematic evaluations of these initiatives to counter online radicalisation. The objective is to measure their real effects and impacts. As with online initiatives in other policy areas, such as road safety or suicide prevention, ensuring that the devices mobilized reach the target audiences is essential for them to be effective. (European Commission, 2024)

However, the adoption of draconian laws, where political control over online censorship is exercised, represents a considerable danger to individual freedom. In a state governed by the rule of law, the only competent authority to decide what is legal or not is the judge. When repressive laws such as the European regulation of mid-2022 against radicalisation are put in place, the presence of the judge is not systematic, which poses a real problem for fundamental freedoms. (Arte, 2024).

Finally, in my view, the effective strategy to counter terrorist propaganda is not necessarily to remove content, but rather to educate users to develop critical thinking. The aim is to provide them with the information and assistance necessary to understand this content, as well as to communicate to them the truth about terrorist organisations and their objectives. Therefore, the key to countering this radicalization, whether it manifests itself online or offline, lies in the human factor. This prospect is encouraging because terrorism is diametrically opposed to humanity; Thus, strengthening humanity is the best way to fight terrorism.

Indeed, let us not forget that although the internet can indeed be considered as an incubator of radicalization, it is interesting to note that being radicalized does not necessarily lead to violent radicalization, i.e. to taking action.

Techniques for detecting and neutralising online radicalisation

Countering online radicalisation is a complex challenge that requires the use of advanced cybersecurity techniques. Online platforms and authorities are working together to develop and apply technologies that can detect and neutralise extremist content and behaviour.

First, the monitoring of online communications is a crucial aspect of cybersecurity in the prevention of radicalization. Authorities must be able to monitor internet exchanges to detect signs of radicalisation and identify individuals involved in these activities. This requires sophisticated technological tools and close cooperation with internet service providers and different social media platforms to access relevant data while respecting users' right to privacy. In addition, data analytics plays a crucial role in detecting suspicious behavior online. (Borelli, 2024). Data analysis algorithms can be used to spot patterns of behaviour associated with radicalisation, such as visiting extremist websites or interacting with radical individuals. This analysis can provide valuable information to authorities to target their prevention and response efforts.

Nevertheless, according to some researchers, alliances formed in the regulatory network reveal cooperation that is often implicit and tinged with underlying resistance. Recent revelations about Edward Snowden's mass surveillance practices of Western intelligence services have prompted social media companies, concerned about their financial interests, to be reluctant to enter any partnership that could damage their reputations. Indeed, some "cyberactivists", committed to self-regulation of online communities, collaborate with private security companies linked to the authorities, while others strongly reject any perceived compromise. These tensions between cooperation, mistrust and rivalry lead to many dilemmas in terms of coordination, in an institutional environment where no single actor holds normative supremacy. (Meidinger, 2009) For example, tougher legislation against the glorification of terrorism in some countries has met with strong opposition from online freedom of expression advocates, who are equally strongly opposed to hate speech (Islamic, left-wing or right-wing extremists, etc.) At the same time, some states have opted for a partnership with social media platforms rather than strengthening legislation. In response to these pressures, platforms have tightened their free speech policies.

Second, automatic detection algorithms are the first line of defense against the spread of extremist content. These algorithms analyze keywords, phrases, images, and videos to identify elements that are characteristic of radical speech. (Kotliar, 2020) For example, specific keywords and phrases associated with radical ideologies can be automatically spotted by content filtering systems. Images and videos are also scrutinized for symbols and gestures typical of extremist groups. This method allows for large-scale, real-time monitoring of content shared on social networks.

In addition, artificial intelligence (AI) and machine learning also play a crucial role in detecting online radicalisation. Predictive models, built from the analysis of historical data, can identify online behaviors that pose a risk of radicalization. Neural networks are used to process large volumes of data and spot subtle patterns of radicalization. (Arte, 2024).

Through AI, social network analysis is essential to understand the spread of radicalization online. Social media mapping techniques make it possible to identify key "influencers" and critical nodes in the networks for the dissemination of extremist content. Proactive monitoring of online activities, which includes tracking interactions and engagements on platforms, helps detect early signs of radicalisation. By observing behaviors and interactions, analysts can identify individuals who are beginning to engage with radicalizing content and intervene before radicalization progresses.

Finally, another possible technique is that filtering and blocking technologies are deployed to prevent the spread of radicalizing sites and information. Content filters, which rely on blacklists and behavioral patterns, can automatically block access to websites and forums associated with extremist groups. In addition, the use of blockchain to ensure data integrity and prevent content manipulation is an emerging approach. Blockchain makes it possible to create immutable records of online activities, making it more difficult for disinformation and radicalizing content to spread. (Winter et al., 2021)

However, as said earlier, it is important to consider the ethical implications and challenges involved in implementing these technologies. Increased surveillance of online activities raises questions of privacy and freedom of expression. Automated detection and filtering systems can also produce false positives, leading to the censorship of non-radicalizing content. It is therefore essential to find a balance between security and individual rights. Transparency policies and redress mechanisms must be put in place to ensure that cybersecurity measures comply with human rights standards.

As a result, countering online radicalisation requires a multifaceted approach, combining advanced cybersecurity technologies, effective policies, international collaboration and increased awareness. By continuing to innovate and collaborate, societies can better protect their citizens from the dangers of online radicalisation and promote a safer and more resilient online environment.

Continuous research and technological development are needed to address the rapidly evolving methods of online radicalisation. Extremist groups are increasingly using sophisticated technologies and encrypted communication platforms to evade detection. Let's now analyse the initiatives put in place by Belgium to fight online radicalisation, and identify the key strategies that can be put in place at the European level.

Cybersecurity and strategies to combat radicalisation in Belgium: Possible avenues?

In the fight against online radicalisation, cybersecurity plays a crucial role in ensuring the protection of digital infrastructure and monitoring suspicious activity. Governments and security agencies must deploy proactive measures to counter these emerging threats. In particular, Belgium has put in place many strategies to try to curb this phenomenon.

In Belgium, several initiatives have been put in place to strengthen cybersecurity and fight online radicalisation. The Cybercrime Center (CLCI) is at the forefront of these efforts, working closely with security agencies to monitor suspicious online activity and investigate cybercrimes related to radicalization. This collaboration allows the Belgian authorities to stay ahead of the curve in the fight against online radicalisation by identifying and neutralising potential threats before they materialise. (Center for cybersecurity in Belgium, 2021)

In addition, public-private partnerships have been established in Belgium to strengthen its capacity to deal with cyber threats. The CLCI, established in collaboration with technology companies and government agencies, plays a central role in this collaboration. The CLCI acts as a centre of excellence in cybersecurity, providing technical expertise, training and coordination of efforts between the public and private sectors to detect, prevent and respond to cyberattacks and online radicalisation. This collaborative approach allows for better use of resources and a more effective response to emerging threats.

In addition, Belgium has launched several awareness programs to educate citizens about online risks and promote safe behaviors on the Internet. These programs are aimed at different audiences, from young people to companies to security professionals, with the aim of raising awareness of cyber threats and strategies to protect themselves from them. For example, awareness-raising campaigns are organised in schools to raise awareness among pupils about the dangers of online radicalisation and encourage responsible use of the Internet, as well as the PRE-RAD unit, which is part of the non-profit organisation Bravvo and is supported by the prevention service of the City of Brussels, plays a crucial role in the prevention of violent radicalisation. By providing support and resources to young people, their families and Brussels associations, it aims to offer preventive support and intervene at the first signs of radicalisation. (Wallonia-Brussels Federation, 2024)

At the European level, an initiative like the one launched in Belgium to raise awareness of online risks and promote safe behaviour on the Internet could be developed. The European Union could facilitate the sharing of best practices among member countries, coordinate continent-wide awareness campaigns, develop training programmes for security professionals, encourage public-private partnerships and provide financial support to member states for the implementation of these programmes. For example, this could take the form of experience-sharing platforms, common guidelines for awareness-raising campaigns, cybersecurity training sessions for security guards, tax incentives for companies collaborating on awareness-raising initiatives, and grants for national online prevention projects.

By implementing these measures, the EU would play a key role in promoting responsible and secure use of the internet across the continent.

Despite these efforts, Belgium still faces persistent cybersecurity challenges. Coordination between different actors, including government agencies, private companies and civil society, remains a major challenge. Closer collaboration and better coordination of efforts are needed to ensure an effective response to cyber threats.

Moreover, at the European level, the protection of citizens' privacy (GDPR) is an important concern in the fight against online radicalisation. Surveillance and data collection measures must be balanced with respect for the fundamental rights to privacy and freedom of expression.

It is essential to put in place appropriate safeguards in Europe to prevent abuse and to ensure that cybersecurity measures comply with ethical and legal standards. (Schunemann et al., 2017)

Finally, adapting to new technologies remains a constant challenge for the Belgian and European authorities. Cybercriminals and extremist groups are continually evolving their tactics and techniques to circumvent existing security measures. Therefore, it is essential to stay on the cutting edge of technology and invest in the research and development of new solutions to counter emerging threats.

It is clear that by combining these efforts, Belgium is working to ensure the safety of its citizens while fighting online radicalisation and strengthening cybersecurity. This comprehensive approach reflects the recognition of the complexity of this challenge and the resolute commitment to address it with determination and cooperation. As part of the Action Plan against Radicalism (Plan R), initiated in 2006 and regularly revised to adapt to the evolution of the terrorist threat, an inclusive and coordinated approach is adopted to prevent radicalisation and violent extremism. By integrating different dimensions of prevention, this plan aims to mobilise all relevant actors, including social, educational and security services, for a holistic and much more effective response. (Dumoulin, 2021).

At the European level, this approach could be strengthened by increased collaboration between Member States. Close coordination of initiatives to prevent online radicalisation, combined with regular exchanges of best practices and data, would maximise the effectiveness of the efforts. In addition, harmonising international policies and strategies in this area would help to strengthen the security and resilience of the entire European Union in the face of this persistent threat.

***

In conclusion, countering online radicalisation is a complex and multifaceted challenge, where individual, social and technological factors interact to influence national security and social cohesion, especially in societies characterised by cultural and religious diversity. This threat transcends national borders and requires a comprehensive, integrated and collaborative approach. The review of Belgian cybersecurity initiatives offers an interesting model for addressing this challenge, highlighting the importance of public-private partnerships, awareness-raising programmes and close coordination between the different actors, an approach that should serve as a reference at European level.

On an individual level, online radicalization is often rooted in factors such as social isolation, alienation, and identity-seeking. Vulnerable individuals may be attracted to extremist ideologies spread on social media, where radicalized virtual communities form and reinforce each other. These digital platforms provide a borderless space for the dissemination of hate speech and the promotion of violence, underscoring the urgency of adopting effective measures to counter this threat.

On a social scale, social media plays a central role in the spread of extremism online. Recommendation algorithms and the virality of content can amplify the spread of radical discourse, exacerbating tensions and divisions within diverse societies. Therefore, effective regulation of online platforms is necessary to limit the spread of extremist content and promote a safer and more inclusive digital environment.

On the technological front, the rapid evolution of digital technologies presents both opportunities and challenges in the fight against online radicalisation. As authorities strengthen their capabilities to monitor and detect suspicious activity on the internet, cybercriminals and extremist groups are constantly adapting their tactics to avoid detection. Indeed, thanks to the capacity for innovation offered by the Internet, radical groups can adjust their strategies to circumvent restrictions by developing countermeasures, or by moving to digital spaces less subject to regulation. This underscores the need for constant vigilance and continued investment in research and development of new security technologies.

In the face of this growing threat, the Belgian authorities have adopted a proactive and collaborative approach. Initiatives such as the Cybercrime Centre (CLCI) and outreach programmes aim to strengthen the country's capacity to detect, prevent and counter online radicalisation. In addition, Belgium is participating in European efforts to harmonise cybersecurity policies and strategies at the continental level, thus recognising the importance of international cooperation in the fight against this transnational threat.

Going forward, it will be crucial to continue research on the individual, social and technological factors that fuel online radicalisation, as well as the effectiveness of cyber security strategies to counter this threat, bearing in mind that radicalisation does not necessarily lead to violent radicalisation. Issues relating to privacy, international coordination and adaptation to technological developments will continue to be the subject of debate and research. By consolidating existing knowledge and exploring new approaches, we will be able to better understand and respond to this complex threat, ensuring the security and resilience of our societies in an ever-changing digital world.

This raises the question in future research: To what extent can strategies for the prevention of online radicalisation be adapted to meet the specific needs of cultural and religious minority communities, while ensuring effectiveness and fairness in protecting national security and social cohesion?

References

- ARTE. (2024). *Can the EU combat radicalisation online?*, https://www.arte.tv/fr/videos/112597-087-A/l-ue-peut-elle-combattre-la-radicalisation-en-ligne/

- BLANCHARD, G. (2007). *Partisan Political Communication on the Internet: New Practices and Strategies?*, pp. 20-28.

- BJORGO, T., SILKE, A. (2018). *Root causes of terrorism*, in SILKE, A. *Routledge handbook of terrorism and counterterrorism*, p. 57-65.

- BORELLI, M. (2024). *Fighting "terrorism" on social networks: uses of a political category in the discourses of Meta, Google and Twitter*, in *Mots. Les langages du politique*, 134, p. 57-79.

- BUSHER, J. (2015). *The making of anti-Muslim protest: Grassroots activism in the English Defence League*, pp. 142-147.

- CENTER FOR CYBERSECURITY – BELGIUM. (2021). *Cybersecurity strategy Belgium 2.0. 2021-2025*, https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

- COURBET, D., FOURQUET-COURBET, M.-P., & MARCHIOLI, A. (2015). *Social media, regulators of collective emotions*, in *Hermès, La Revue*, 71(1), p. 287-292.

- DUMOULIN, A. (2021). *Belgium and the Fight Against Terrorism*, in *Annuaire français de relations internationales*, p. 139-151.

- EUROPEAN COMMISSION. (2024). *Prevention of radicalisation*, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation_en

- EUROPEAN COUNCIL & COUNCIL OF THE EUROPEAN UNION. (2024). *The EU's response to terrorism*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/preventing-radicalisation/

- WALLONIA-BRUSSELS FEDERATION. (2024). *Network for the Management of Violent Extremism and Radicalism*, https://extremismes-violents.cfwb.be/ressources/carnet-dadresses/#:~:text=Cellule%20PRE%2DRAD%20(Prevention%20of%20la%20radicalisation%20violent)&text=Elle%20acte%20en%20support%20of,the use%20of%20the%20violence.

- FRIEDLAND, N. (1988). *Political Terrorism: A Social Psychological Perspective*, in STROEBE, W., KRUGLANSKI, A.W., BAR-TAL, D., HEWSTONE, M. *The Social Psychology of Intergroup Conflict*, pp. 103-114.

- GRASSEGGER, C. (2022). *How does the European Union deal with the challenges of the fight against terrorism and radicalisation?, in Cahiers de la sécurité et de la justice*, 55, p. 86-97.

- GOODWIN, J. (2006). *A Theory of Categorical Terrorism. Social Forces*, *84*(4), pp. 2027–2046.

- HORGAN, J. (2008). *From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism*, in *The Annals of the American Academy of Political and Social Science*, 618, pp. 80–94.

- HORGAN, J. G. (2017). *Psychology of terrorism: Introduction to the special issue*, in *American Psychologist,* 72(3), pp. 199–204.

- OFFICIAL JOURNAL OF THE EUROPEAN UNION. (2021). *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on combating the dissemination of terrorist content online,* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A32021R0784

- KOTLIAR, D. M. (2020). *The return of the social: Algorithmic identity in an age of symbolic demise*, in *New Media & Society*, 22, p. 1152-1167.

- LAUW, H. W., NTOULAS, A., & KENTHAPADI, K. (2010). *Estimating the quality of postings in the real-time web*, pp. 1-4.

- LINDEKILDE, L., MALTHANER, S., & O'CONNOR, F. (2019). *Peripheral and embedded: Relational patterns of lone-actor terrorist radicalization*, in *Dynamics of Asymmetric Conflict*, 12(1), pp. 20-41.

- MCCAULEY, C., & MOSKALENKO, S. (2001). *Friction: How Radicalization Happens to Them and Us*, pp. 51-86.

- MCKENNA, K. Y. (2007). *Through the Internet Looking Glass: Expressing and Validating the True Self*, in JOINSON, A., MCKENNA, K. Y., POSTMES, T., & REIPS U.-D. *The Oxford Handbook of Internet Psychology*, pp. 34-66.

- MEIDINGER, E. (2009), *Private Import Safety Regulation and Transnational New Governance*, pp. 2-13.

- NEUMANN, P. R. (2015). *Radicalization. Critical Concepts in Military, Strategic, and Security Studies*, p. 9-31.

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

- RANDALL, D. (2019). *The Routledge history of terrorism*, pp. 26-47.

- REICHER, S. D., SPEARS, R., & POSTMES, T. (1995). *A social identity model of deindividuation phenomena*, in *European review of social psychology*, 6(1), pp. 161-198.

- RIVA, G., MANTOVANI, F., CAPIDEVILLE, C. S., PREZIOSA, A., MORGANTI, F., VILLANI, D., GAGGIOLI, A., BOTELLA, C., & ALCAÑIZ, M. (2007). *Affective interactions using virtual reality: The link between presence and emotions*, in CyberPsychology & Behavior, 10(1), pp. 45-56.

- SCHUNEMANN, W., BAUMANN, M. (2017). *Privacy, date protection and cybersecurity in Europe*, pp. 22-39.

- SWANN JR., W.B., & BUHRMESTER, M. D. (2015). *Identity fusion*, in *Psychological Science*, 24(1), pp. 52-57.

- WEIMANN, G. (2005). *How Modern Terrorism Uses the Internet*, in *The Journal of International Security Affairs*, 8, pp. 91-105.

- WEIMANN, G. (2010). *Terror on facebook, twitter, and youtube*, in *The Brown Journal of World Affairs*, 16, pp. 45-54.

- WINTER, C., NEUMANN, P., MELEAGROU-HITCHENS, A., RANSTORP, M., VIDINO, L., & FÜRST, J. (2021). *Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies*, in *International Journal of Conflict and Violence*, *14*, pp. 1–20.

- ZHAW & HES.SO (2022). *Juvenile delinquency in Switzerland. Main results of the 4th wave of the International Juvenile Delinquency Survey*, https://www.hets-fr.ch/media/neqjseng/rapport_national_isrd4_français_def.pdf