

Online Radicalization and Misogynistic Extremism: Case Study of Cyberbullying

inspector Aleksandar Atanasov

Criminal Police, Republic of Bulgaria,

Doctoral Candidate at the Academy of the Ministry of Internal Affairs – Republic of Bulgaria

AlVaAtanasow@mvr.bg

Abstract: *Cyberbullying reflects society's old patterns of violence, now multiplied by technological advancement. The rise of global polarization has amplified misogynistic extremism, sometimes exploited by foreign actors to destabilize democratic societies.*

This case study examines a male perpetrator under 30 who systematically harassed and bullied over 40 women aged 18-40, all social media influencers with high social status and well known and developed profiles.

The methodology relies on qualitative data analysis of open-source information, including academic literature, news articles, and investigative materials, combined with the author's professional experience as a criminal intelligence investigator on this case. The analysis employs criminal psychology profiling, criminology, and criminal intelligence frameworks to examine perpetrator and victim profiles and the crime's modus operandi.

The study finds that the perpetrator's misogynistic behavior is connected to systematic drug use and lifelong problems with women, attacking victims after initial signs of rejection without proper capacity for social orientation and adaptation. The perpetrator victimizes women through dehumanizing thought patterns, targeting the most influential and physically attractive victims, focusing explicitly on their physical appearance and social status. Law enforcement and prosecutors faced major challenges due to non-digitalized legislation and inadequate tools for proper observation and OSINT analysis of connected digital evidence.

Good practices that emerged include effective identification of unknown victims through pattern analysis and leveraging the perpetrator's consistent psychological and behavioral patterns to predict and prevent further victimization.

This report provides a framework for developing policies to counter cyberbullying and strategies to combat misogynistic extremism and online radicalization.

Keywords: *Online radicalization, Misogynistic extremism, Cybercrime investigation*

INTRODUCTION

Cyberbullying is an ongoing trend in the era of global digitalization and the rise of AI. The purpose of this case study is to represent a typical case that involves multiple victims with a major impact on society and partly on some of the victims' lives, for which this criminal act inflicted great emotional and personal damage, and also to represent the problems that law enforcement authorities faced in investigating and developing the case into a lawful courtroom accusation of the perpetrator. The goal of this manuscript is to provide valuable insights and information for lawmakers to address current legislation problems in cases of cyberbullying, law enforcement agencies facing these challenges to detect and apprehend criminals, and NGO officials that provide support for victims.

Cyberbullying prevalence can be observed in the 55% of U.S. students who experienced cyberbullying in their lifetime, of which 27% experienced it in the past 30 days. As for gender differences, girls dominate over boys with a slight difference (Cyberbullying Research Center, 2023). From world data, we can observe that more than 21% of female victims aged 19-25 report distinct emotional disturbances due to cyberbullying. Data from a 2016 study regarding young women showed that the majority, or 56.8% of respondents, had already experienced some form of cyber harassment. About 21% experienced distinct emotional disturbances, while 31% felt anger. Some 20.8% of victims said that they felt helpless, while 20.5% reported feelings of sorrow (Heliyon, 2016).

The phenomenon extends beyond adolescents: according to Pew Research Center, 41% of American adults have experienced some form of online harassment, with 25% reporting severe forms including physical threats, stalking, and sexual harassment — a figure that has nearly doubled since 2014 (Vogels, 2021).

As we can see from the trend data, this wave of harassment affects in greater number the female part of the web, which directly transfers to the element of misogynistic extremism. In this research, we will understand it as an online subculture in which men blame women for their involuntary celibacy — while the majority of incels are non-violent, some members consider themselves to be staunch misogynists and are likely to endorse violence, according to the Europol definition of Incel included in the European Union Terrorism Situation and Trend Report (TE-SAT) 2022 (EUROPOL, 2022).

There is no clear internationally accepted definition for cyberbullying. Different countries adopt it in their national legislation framework or as a specific term of expertise in their field. For example, the U.S. Department of Health and Human Services defines cyberbullying as bullying that takes place over digital devices like cell phones, computers, and tablets — it can include sharing personal or private information about someone else causing embarrassment or humiliation (U.S. Department of Health and Human Services, 2024).

The lack of an internationally adopted legislation framework leaves countries such as Bulgaria in an information vacuum where there is no officially adopted legal term or criminal penalty code that addresses this issue. The definition used for bullying or harassment still follows

the old Soviet legislation framework, written in the analog time before the digital era of computers and internet.

For the purpose of this research, the definition of cyberbullying that we will be using is willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices (Hinduja & Patchin, 2024), which also includes the following elements:

- Willful: The behavior has to be deliberate, not accidental.
- Repeated: Bullying reflects a pattern of behavior, not just one isolated incident.
- Harm: The target must perceive that harm was inflicted.
- Computers, cell phones, and other electronic devices: This is what differentiates cyberbullying from traditional bullying.

This directly transfers into the elements of our studied case and reflects the behavior of the perpetrator studied in this research.

METHODOLOGY

The methodology employs qualitative data analysis of open-source materials, including academic literature, news reports, investigative journalism, and institutional literature from law enforcement agencies. The analysis is informed by the author's direct professional experience as a criminal intelligence officer in the Bulgarian Ministry of Interior, providing operational insights into radicalization patterns and escalation dynamics within the digital domain and working directly on this case from start to finish.

The research framework integrates publicly accessible sources with professional observations derived from operational materials, which cannot be explicitly cited due to ethical standards and confidentiality requirements under Article 198 of the Bulgarian Criminal Procedure Code (pre-trial investigation secrecy) and personal data protection regulations and ethical standards. This case study approach synthesizes patterns from an investigation conducted in 2025 that reflects current trends in interpersonal crime escalation and radicalization pathways from events that developed over the last 3 to 4 years.

This methodology offers the advantage of bridging academic analysis with field-level intelligence, providing perspectives typically inaccessible through open-source research alone. The limitation lies in the inability to verify certain operational observations through citation, requiring reader reliance on the author's professional credibility. However, all analytical claims supported by open-source data are appropriately referenced, ensuring transparency where confidentiality constraints permit.

PROFILE OF THE PERPETRATOR

The perpetrator in the present case study represents a specific typology of cyberbullying offender whose criminal behavior is directly determined by severe psychopathological processes with developed antisocial personality structure. He was chosen for this research as a unifying example of a digital cyberbullying criminal, especially because of his strong misogynistic attitudes shown through the work with him on this case, which resulted from his poor life choices and lack of skills to achieve his goals to be successful with women in a lawful and morally acceptable way — this was turning him into a violent digital offender who transfers his objects of affection into victims after he faces rejection.

Background and developmental trajectory

The subject demonstrates early indicators of deviant development — behavioral problems emerging during adolescence, including substance use (cannabis) initiated during his school years. Despite completing secondary education and achieving a period of relative social stability during extended residence abroad (approximately 7-8 years), the perpetrator failed to establish lasting social bonds, intimate relationships, or family unit. Upon return to the home country, substance use resumed and progressive social deterioration accelerated according to his own statements. In this period he constantly used cannabis and was experiencing adaptation problems. He states that he had only one girlfriend who was with him for several years and left him of her own will. After that he did not managed to win her back and learned that she was intimate with a friend of his — this fact bringing him extra hurt and anger towards her and females as a whole. After this breakdown, he engaged in sexual contacts with males of his own will, for which he feels further ashamed, and did not manage to build a bond with another female on the same level such as his ex-girlfriend indicating a change in behavior and appearance after the break-up.

Clearly, we can look at the pattern of systematic narcotics use, major life breakdown event followed by a decision that brings shame to the individual without a proper mechanism of re-adaptation and balancing behavior that can restore his personal self-worth — which escalated into misogynistic behavior against females. It is important to mention that after these events, the perpetrator purposefully leaked private intimate sexual photos of him and his ex-girlfriend online through social media in his own act of vengeance against her. Unfortunately, she never brought this information to the police or filed a case for this typical revenge porn modus operandi.

At the moment of arrest, the perpetrator was working as a security guard in a government-owned company under the Armed Forces of Bulgaria, tasked to provide security for military-grade areas.

Psychological profile

The forensic evaluation establishes diagnoses of Paranoid Schizophrenia (F 20.0 per ICD-10 classification — a chronic psychotic disorder characterized by systematized delusions, typically of persecutory nature, with relatively preserved cognitive functioning) and Mental and Behavioral Disorders due to Cannabis Use — Harmful Use (F 12.1 per ICD-10 — substance use causing

demonstrable psychological damage, comorbid with the primary psychotic illness). It is also important to mention that the perpetrator experienced a divorce of his parents during his teenage years, which can bring different and unknown effects into his perceptions of normal relationships between man and woman.

The personality orientation is defined as paranoid-hostile with avoidant adaptation style. Dominant characteristics include:

- Schema of threat and vulnerability as primary interpretive framework towards women;
- Distress-oriented affective disposition (anxiety, anger, shame) with low frustration tolerance — his inability to comprehend rejection;
- Social functioning deteriorating toward complete isolation — representing pathological coping with internal tension — his inability to self-reflect and overcome distress;
- Strongly expressed aggressive tendencies that are pathologically motivated towards women;
- Aggression functioning as secondary symptom — a coping mechanism for managing intensive affective distress, not a result of typical antisocial disorder.

Critically, the aggressive behavioral pattern shows marked internal conflict: elevated scores for hostile attitudes (64%), aggressive distrust (90%), irritability (72%), and verbal aggression (69%) coexist with significant guilt following aggressive acts (66%). This indicates the perpetrator experiences shame, self-blame, and internal suffering as consequence of his own behavior — distinguishing him from classical antisocial offenders who typically demonstrate absence of remorse and placing him in the typical radicalization pattern of the lone wolf with developed mental health issues, where 43% of such offenders are found to have psychiatric disorders (Gill et al., 2014). This pattern is consistent with findings from research on active shooter incidents, which similarly identifies mental health factors as a significant component in the radicalization trajectory of lone-actor violence (Atanasov, 2017).

Criminal behavior mechanism

The cyberbullying conduct in this case constitutes compulsive, indirect externalization of delusional persecution fears and lack of healthy patterns to deal with the initial trauma. First, due to his lack of success with his girlfriend who left him and the lack of skills to overcome this life event, and second, due to his lack of capacity to attract a female partner desired by him.

Within this delusional framework, the perpetrator engaged in sending threats and sexually explicit uncensored content to unknown female victims via social media platforms, whom he initially contacted as potential romantic partners. This targeting of women was incorporated into his broader delusional system rather than emerging from organized misogynistic ideology — the misogynistic element follows after their rejection of his friendship and company and can be seen

through the words he used to victimize them, such as "they are powerful, they are junk, they don't need protection." The utilization of multiple fake profiles provided an illusory sense of power and control over his victims — compensating for powerlessness experienced in real life in meeting them and sharing life experiences.

The psychological experience of cyberbullying behavior represents externalization of internal psychological warfare and lack of skills for social adaptation due to his systematic drug abuse, which potentially developed into psychopathological harmful behavior and his arrested personal development — leading to his misogynistic radicalization. The act provides temporary relief from tension and a sensation of control, followed by intensive suffering that reinforces self-blame and deepens isolation — creating a self-perpetuating cycle of wanting and hate females.

Criminological assessment

From a criminal intelligence perspective, this perpetrator type presents distinct characteristics:

1. **Predictability** — behavior is psychotically motivated, often following the criminal logic that he will contact high-value online influencers who will reject him afterwards due to his poor communication skills and personal characteristics, which will result in a massive offensive campaign by him against the victim. This process will repeat on a larger scale with other females.
2. **Escalation risk** — delusional system can incorporate new targets; perceived persecution can intensify, potentially increasing severity of threatening behavior. Usually, the perpetrator escalates from giving commands, to using hate speech, afterwards to applying systematic pressure with multiple accounts, messages and tools for digital presence and stalking of the victim's online activity, to displaying weapons, drugs and demanding the victim lock or delete their account or he will not stop.

The forensic conclusion establishes that the perpetrator lacks mental capacity to comprehend the meaning and significance of criminal proceedings against him, cannot participate meaningfully in the legal process, and cannot bear criminal responsibility in the conventional sense. The recommended intervention is compulsory psychiatric treatment rather than penal sanction according to the Bulgarian legislation framework.

Typological classification

This case represents an intersection of mental illness and cyber-enabled crime where the perpetrator is simultaneously offender and victim of his own psychopathology. The cyberbullying behavior, while causing genuine harm to victims, emerges from psychotic disorganization caused by life events and the use of drugs, which can present a typical pathway of radicalization into structured extremism and calculated criminal intent that has been observed in other major cases in the country, such as that of Ahmed Musa — an Islamic extremist who radicalized after the death

of his daughter who drowned in the sea while wearing full Islamic clothing covering her body, an event perceived by Ahmed Musa as unlocking his radicalization. This confirms the profile as a typical radicalization pattern where individuals progressively adopt extremist behavior in the context of their own personal deficits in major life events and the lack of ways to achieve their goals in a lawful manner. The radicalization pattern here is produced by pathological mental processes rather than emerging into external influence on his victims, which is a typical mechanism of violent offenders in criminal psychology (Douglas & Olshaker, 2017). After all, all he wanted was to be with a young, beautiful and valued woman, but due to his lack of personal skills and characteristics, he victimized all of the women he contacted due to their rejection of him for his lack of skills and value to offer in the dating market.

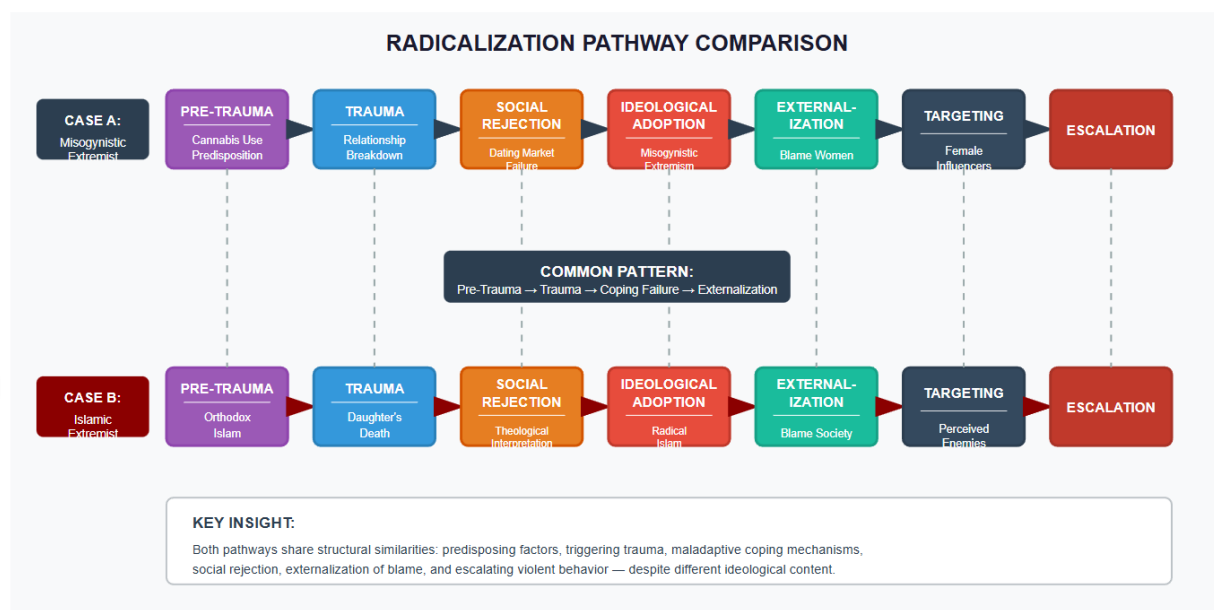


Figure №1. Comparison of the radicalization pattern in of two different cases.

It is of major importance to mention that a year ago, when the perpetrator was involved in another criminal case, the psychopathological expertise concluded that his behavior was conscious and he was criminally liable. In this period his criminal activity as a cyberbully was ongoing, so here the question is directly connected to the psychological expertise applied to the case — because in conclusion we have a person who was perpetrating a criminal offence over a long period of time, undergoing two psychopathological expertises that found him both criminally liable and later not criminally liable after a period of time. In both cases it is clear that his model of radicalization and actions persist.

PROFILE OF THE VICTIMS

As mentioned in the abstract, the victims of our cyberbully are over 40 women aged between 18 and 40 years old, some of them falling victim to the perpetrator before turning 18. All of them are social media influencers with high social status and well-known, developed social

media profiles, ranging from persons with average social media popularity to those who are well known within the country. For average social media influencer in the context of this term as used in our current manuscript must be understood — a person who is well known on the level of the city or region; above average are persons well known on a higher level in different communities, circles and areas of the country. It is important to mention that most of the victims of the perpetrator are well connected to the primary city of residence of the perpetrator, which is an important factor, because as was well observed, initially he wanted to start a romantic relationship with them that eventually ended in cybercrime.

Backgrounds of the victims

Most of the victims of our perpetrator come from a middle to high social background, with families working in middle-class professions in the public or private sector. Some of them come from families with a higher socio-economic background. Some of the victims are business owners or official influencers — promoters of different medical or beauty products, others are graduated medical personnel or from profiles connected to year-long bachelor and master education.

Some of the victims are engaged to other male partners such as boyfriends or fiancés, which is not publicly shown in their profiles. It is interesting to observe that our perpetrator avoided profiles that are publicly perceived as belonging to a female with a partner. This is due to the fact that, as he mentioned in one of the interviews, he does not want conflict or confrontation with other males. In part of his public threats it can be seen that he does not fear, when he is behind a screen, to offend or threaten other males who entered the public conversations as defenders of the females, but as history shows, when a female mentions she has a boyfriend in the conversations, this does not stop him from continuing his online aggression towards the victim.

Most of the profiles do not show a direct family connection with other male figures and the perpetrator seems not to include in his actions the consequences of revenge actions from fathers in this paradigm.

Type of the victims as phenotypic characteristics and social profile

If we look at "what type of females" are victimized by the perpetrator, we must come to the conclusion that he purposefully chooses the "classical model type" that can emerge if we look at the most common female fashion models. An example for this is an Instagram profile connected to a high-level make-up artist who produces many pictures of her clients, but the female artist herself was not bullied because he does not feel attraction towards her — this is because no matter her beauty, she does not fall into the same "classical model body type." In this case he bullied all of the clients of this Instagram make-up page and when he was confronted by the make-up artist, a woman herself but not with this victimized body look and type — he just almost ignored her from his attention.

No matter the age of the victims, their typical body type resembles a thin, short or tall woman with white skin, well invested in make-up or cosmetic procedures. They represent

themselves in high-level photos and maintain an image of important, well-known persons who travel a lot and possess a luxury life.

Response of the victims to the actions of perpetrator

The typical first response of the victims was to ignore the perpetrator. After that, when he persisted, they blocked him, some of them engaging in a conversation that can be described as deterrent, showing him directly that they do not possess interest in him. After the initial ignore, negative comments and block of the perpetrator, they fall into one of the following categories:

- **Trying to cooperate with him.** Some of them tried afterwards to find common language and to stop him by will and normal conversation. This happens at the stage where he had already registered multiple accounts that were blocked and tried to catch their attention with comments in the first stages of indirect aggression. After that, when he faced their unwillingness even in a cooperative manner and escalated the conversation with threats, the victims started to fear real danger because of him and his actions and that they did not manage to find an understanding person and behavior that can be perceived as normal on the other side. In these cases, his obsessive behavior escalates without restraint, so their cooperative behavior transforms into one of the other options.

- **Totally blocking and ignoring him.** A small part of the victims just totally ignored and blocked him without leaving any channel of communication, which seemed to be the safest way out of his obsessive and aggressive behavior even when it escalated to other levels of online aggression. This type of victims just implemented the policy of zero conversation with him and only applied the restrictions of social media until he found another victim and transferred somewhere where his attempts to gather attention were met with response.

- **Using threats and counter-violence.** Some of the victims responded with aggressive behavior towards the perpetrator, not in the direct life-threatening way as he did, but in a more civilized way which only brought more attachment from the perpetrator to them and more unwanted and unnecessary attention, continuing their online struggle to deter the perpetrator by using counter-force.

VICTIM PROFILE MATRIX

CHARACTERISTIC	DESCRIPTION
Total victims	Female social media users (40+)
Age range	18–40 years (some victimized as minors)
Social background	Middle to high socioeconomic status
Occupation	Various professions across public and private sectors
Online presence	Regional to national social media influencers
Physical profile	Consistent phenotypic targeting pattern ("classical model type")
Visible relationship status	Predominantly no visible male partner; targeting continued after discovery of existing relationships
Geographic connection	Majority linked to perpetrator's primary city of residence

Figure №2. Victims profile matrix

Overall, no matter the way of responding to the perpetrator, all of the victims fell to his aggressive and hateful behavior, experiencing major stress and some of them fear for their lives — a pattern consistent with research showing elevated suicidal ideation among cyberbullying victims (Hinduja & Patchin, 2010). This disrupted their peace and social image, incorporating fear in their families, as in some cases other family members of the victims were directly involved and targeted as victims of his cyber misogynistic extremism.

MODUS OPERANDI OF THE CRIME

First phase of the modus operandi of the crime includes the initial contact from the perpetrator to the victim. As was mentioned, he targeted his specific profile of female online influencer victims of the "model type" with high social influence and followers whom he perceived as physically attractive and as a potential romantic match. This targeting happens through the Meta platforms of Instagram and Facebook. His primary chosen platform between the two is Instagram where most of the females post more attractive and professional photographs compared to their Facebook social media profiles. Of course, a major factor is also the profile's status as open or closed in choosing his victims, with the main criterion being access to photos that can stimulate his inner fantasies.

Second phase of the modus operandi is the initial contact through comments and partly through messages. His preferred way of communication is through comments on social media posts of their pictures where he writes playful or romantic comments towards them. After that he contacts them for direct messaging or sends a request which gets refused or ignored, along with his public comments.

This sparks the **third phase** where he starts to victimize his victims with bullying and threats. Here he starts to write aggressive comments connected to their physical appearance and their social status, he attacks them with hate speech connected to their looks and their behavior with males, describing them as ugly and as whores. It is important to mention that in his interviews he did not mention feeling guilty about this and described them as "persons who don't need protection," because "they have power over many other men and they use this power to their advantage." In this phase, if he gets attached to a victim due to her reciprocated attention, he escalates even more.

Going to the **fourth stage** where he starts to post images of pictures of the victim merged with his genitals, or in a sexual way using pictures of his old girlfriend where he is intimate and sexual with her and adding a picture or text of his victim. Basically, he makes collages with a female body that he is intimate with and adds the credentials of his victim to make the impression that he was intimate with this woman, which asserts his dominance and makes her image unworthy and damaged by this false influence due to the perpetrator's collages. His escalation continues to

posing with guns and knives with direct verbal threats that he will find and kill his victims, even using words such as "I want your blood on my knife" to one of them.

In this fourth stage he also uses his scheme of creating multiple social media profiles due to a weakness in one specific email domain where he can create multiple emails without second verification. Using this specific online email domain he creates and verifies over 30 different profiles after each time he is blocked. Basically, he creates a new one that gets blocked, and a new one, making the perception of infiniteness and putting pressure on the victim that they cannot stop his bullying and threats to their profiles.

On the **fifth stage** of the modus operandi he usually wants the victim, after his psychological warfare has emerged and is winning, to "close her profile" — which action he afterwards presents as a victory. In some of his posts on his profiles he writes that he made X number of victims, using their names, close their profiles due to fear of him and due to his manly actions to subdue them. In this manner he also posts stories where he poses as a winner of street duels, implementing fear in others — including men — and winning some arguments or fights, trying to sustain and create an image of a hard and tough guy. For this image he regularly posts pictures with marihuana and a balaclava in combination with machetes, knives and a gun. The last one he truly owns as he possesses an unregistered gas-signal pistol (which can be converted to a lethal shooting pistol with proper intervention), marihuana that he truly possessed in the past and used as a drug, and a machete and knives that he actually owns.

On this fifth stage of the modus operandi, after the victim closes their profile or goes totally silent to him, he usually continues to another female or to a connected female to the same victim, putting his energy towards wanting to enforce dominance over the next woman, bullying whole communities of girls connected through friendly or family relationships.

In the work on the case it was concluded that for this he used only his mobile phone or a combination of mobile phones where he also saved pictures of his victims, not only for his collages but also possibly for an obsession with them due to his fantasies, because such pictures of them were found alongside many pornographic materials connected to his personal sexual experiences and the mentioned above perception of a criminal lifestyle connected to drug usage.

As for the temporal pattern across the different stages, the perpetrator's behavior is clearly dependent on his personal experience, his attraction to the victim, and her response in terms of engagement options. He spent more time with victims who were in some way active and responsive to his aggression or behavior and brought him attention that fulfilled his inner fantasies, needs, and affections — keeping him engaged in the way a video game with unknown results would, allowing him to express his power and dominance or to reinforce his hope that he could manage to win or subdue some of his victims in a manner desired by him.

POLICE CHALLENGES AND GOOD PRACTICES

The main police investigation challenge in this crime was to prove the crime itself. The lack of a digital legislation framework puts the deeds under the influence of the old Soviet legislation framework that was written in a time for and under the hypotheses of a non-digitalized world where computers were only known and used for space exploration back then. It is important to notice that to prove "threats to the life and health" of the victim, our legislation framework requires having "reasonable circumstances to carry out the threat" — which requires at least some direct action in real life towards the victim. This was one of the main legal loopholes that the lawyer of the perpetrator used, because when he asked him "have you ever met some of your victims" — he replied — "no, I have only seen some of them in the center of the city, but they never knew."

The lack of a proper legislation framework to address this type of crime is a major problem, and as many of the victims told the police "we thought that there was nothing you can do about it, so that's why we didn't report it to the police" — which is a well-known observation of our current reality in Bulgarian law.

The other critical issue is his current status of not being competent to be held accountable. A year before his current arrest he was attacked by males who saw him in the city center and recognized him as the bully of our over 40 victims and attacked him. He escaped but used his pistol as a weapon of defence. In this situation, after the psychopathological expertise, he was declared competent to be held accountable by the law. Right now, a year later, in this expertise he is declared not competent. Also, regarding some of the psychological analyses by experts who are not familiar with the effects of radicalization and the elements of criminal psychology, the author of this manuscript as a doctoral candidate in criminal psychology and law enforcement officer in the heavy crimes unit in the last 5 years tends to disagree.

The main problem with establishing mental competency for criminal prosecution lies in the methodology employed by forensic psychiatric experts. These professionals typically apply standardized evaluation protocols designed for clinical settings where patients present genuine symptoms without deceptive intent. However, when assessing criminal offenders, this approach becomes problematic. Criminal psychology operates within different dimensions and recognizes patterns that are not directly addressed in consultative psychology and psychiatry — the disciplines applied in this perpetrator's evaluation. In fact, during multiple interview sessions, the perpetrator purposefully provided false answers regarding the details of events and his own actions, thereby supporting a distorted perception in the psychological and psychiatric analysis. This manipulation succeeded because the experts were not trained to anticipate or detect deception strategies commonly employed by criminal subjects. When forensic experts work exclusively within their clinical framework, they encounter mentally ill patients who are not criminals and have no motivation to deceive. To work effectively with criminal populations, these experts must also integrate principles of criminal psychology — including deception detection, manipulation recognition, and behavioral consistency analysis — to produce assessments that cannot be compromised by the deliberate actions of the subject being evaluated.

The main intelligence challenge was to detect and find the current location of our perpetrator after we easily established his identity due to the resources used by the victims to recognize this person as their attacker and due to the fact that a couple of times he posted his personal pictures posing with a gun or being sexual with his ex-girlfriend.

His internet misogynistic extremism was practiced while he was changing more than 4-5 different locations in Bulgaria and one outside of the European Union. For this period of time, due to fear of his actions and due to intervention of his family, he was sent to the countryside where he worked as a security guard at a military facility in a company owned by the Bulgarian Armed Forces. His records of residing or even buying online orders were connected to other locations, but not one of them was connected to this countryside village.

As good practices from this case we can note the importance of proper OSINT intelligence and digital intelligence and investigation that was required to connect all of the dots of his online profiles and activities, and the support of the victims in this investigation who were assured and whose trust was gained that it is important to document with a screenshot and a report every current and other action of his, especially to profiles that were active and regularly used in the past weeks or days by the perpetrator.

CONCLUSION

This case study examined a perpetrator of cyberbullying whose behavior exemplifies the intersection of psychopathology, substance abuse, and misogynistic radicalization. The analysis reveals several critical findings with implications for law enforcement, mental health professionals, and policymakers.

The perpetrator's trajectory demonstrates a recognizable radicalization pathway: personal trauma (relationship breakdown), substance abuse (cannabis), progressive social deterioration, and externalization of internal distress through targeted aggression against women. His victimization of over 40 female social media influencers followed a predictable five-phase modus operandi, escalating from romantic approach to death threats and sexual harassment. The psychological profile indicates paranoid schizophrenia with comorbid cannabis use disorder, yet his criminal conduct maintained consistent logic and targeting criteria throughout, raising questions about the application of forensic psychiatric assessments in cases of extremism or a legislation framework gap.

The victims shared common characteristics: high social visibility, "classical model type" physical appearance, and middle-to-high socioeconomic background. Regardless of their response strategy — cooperation, total blocking, or counter-aggression — all victims experienced significant psychological harm, with fear extending to their families.

The broader implications of cyberbullying victimization cannot be understated. Research demonstrates that adolescents who experience cyberbullying are more than four times as likely to report suicidal thoughts and attempts compared to those who have not experienced such

victimization (Arnon et al., 2022). This association persists even when controlling for other risk factors such as family conflict and in-person bullying, underscoring the independent psychological toll of cyber-enabled harassment.

Law enforcement faced substantial challenges due to Bulgaria's outdated legislative framework, which requires "reasonable circumstances to carry out the threat" for prosecution — a standard designed for physical-world crimes that fails to address digital harassment. The perpetrator's contradictory forensic assessments — declared competent one year and incompetent the next while committing the same ongoing offenses — highlight systemic weaknesses in applying psychiatric expertise to cases involving radicalization dynamics.

Good practices emerging from this investigation include the critical importance of OSINT intelligence for establishing perpetrator identity and location, systematic documentation of all digital evidence by victims, and leveraging the perpetrator's predictable behavioral patterns for anticipating future targets. Victim cooperation proved essential when trust was established through professional assurance that law enforcement action was possible.

This case provides a framework for understanding how individual psychopathology can manifest as misogynistic extremism in digital spaces, and emphasizes the urgent need for legislative modernization, specialized forensic training in radicalization dynamics, and coordinated victim support mechanisms as a full holistic approach with a digitalization of the police force and the current legal framework to address the challenges of the digital domain.

REFERENCES

Arnon, S., Brunstein Klomek, A., Visoki, E., Moore, T. M., Argabright, S. T., DiDomenico, G. E., Benton, T. D., & Barzilay, R. (2022). Association of Cyberbullying Experiences and Perpetration With Suicidality in Early Adolescence. *JAMA Network Open*, 5(6), e2218746. <https://doi.org/10.1001/jamanetworkopen.2022.18746>

Atanasov, A. (2017). *Analysis of Active Shooter Incidents*. Zenodo. <https://doi.org/10.5281/zenodo.17560680>

Cyberbullying Research Center. (2023). *2023 Cyberbullying Data*. <https://cyberbullying.org/2023-cyberbullying-data>

Douglas, J. E., & Olshaker, M. (2017). *Mindhunter: Inside the FBI's Elite Serial Crime Unit*. Gallery Books.

EUROPOL. (2022). *European Union Terrorism Situation and Trend Report (TE-SAT) 2022* (p. 50). https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

Gill, P., Horgan, J., & Deckert, P. (2014). Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences*, 59(2), 425–435. <https://doi.org/10.1111/1556-4029.12312>

Hinduja, S., & Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), 206–221. <https://doi.org/10.1080/13811118.2010.494133>

Hinduja, S., & Patchin, J. W. (2024). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (3rd ed.). Corwin Press.

Karovic, M. (2023). *Cyberbullying Statistics*. DataProt. <https://dataprot.net/statistics/cyberbullying-statistics/>

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. <https://doi.org/10.1037/a0035618>

U.S. Department of Health and Human Services. (2024). *What Is Cyberbullying*. StopBullying.gov. <https://www.stopbullying.gov/cyberbullying/what-is-it>

Vogels, E. A. (2021, January 13). *The State of Online Harassment*. Pew Research Center. <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>

Zalaquett, C. P., & Chatters, S. J. (2014). Cyberbullying in college: Frequency, characteristics, and practical implications. *SAGE Open*, 4(1), 1–8. <https://doi.org/10.1177/2158244014526721>