NBP. Nauka, bezbednost, policija
Published by
University of Criminal Investigation and Police Studies
2026, Vol. 31, Issue 1, pp. 20–33
https://doi.org/10.5937/nabepo31-60502
Original Scientific Paper

Liking Harm, Feeling Fine: Crowd-Cruelty Comfort and the Normalization of Digital Aggression

Dijana Sulejmanović[1], **Irma Kadić**
Independent Researchers, Bihać, Bosnia and Herzegovina

Submitted: 2025-07-29 • Accepted: 2025-08-21 • Published: 2025-11-07

Abstract: This article explores the psychological processes and behavioural practices that result from an individual's involvement in online aggression, with a particular focus on social reinforcement processes in virtual communities. Theoretical frameworks well-grounded in the psychological literature, such as deindividuation, moral distancing, and digital disinhibition, will help identify general characteristics of online aggressors and specific behaviours such as endorsing the group through likes, shares, and supportive comments.

In an effort to capture the complexity of the online space, an innovative and explanatory concept called Crowd-Cruelty Comfort (CCC) is presented – as a new theoretical framework that describes how individuals have reduced moral discomfort and increased psychological comfort when engaging in harmful or supportive behaviours in the digital space. This concept explains the growing normalization of online aggression through well-studied concepts and mechanisms such as moral mitigation, diffusion of responsibility and suppression of empathy, which were previously identified and explained in the literature, but are now observed in a new context, with new meanings and new consequences that they leave in virtual reality.

CCC describes how individuals psychologically process that the harmful or destructive behaviours they engage in are in fact morally justified – and therefore can believe they are not to blame for the behaviour and can maintain a positive self-image. The implications of this concept are discussed with respect to digital ethics education, prevention strategies, and intervention programs aimed at mitigating the spread of online harm.

Keywords: online abuse, digital aggression, cyberbullying, Crowd-Cruelty Comfort.

INTRODUCTION

In modern digital society, an increasing part of social interaction is being moved to virtual spaces, which brings with it a number of new forms of deviant behaviour, among which digital aggression occupies a special place. Although traditional forms of violence still occur in physical space, the virtual world enables specific patterns of psychological and verbal aggression, often without physical contact, but with serious consequences for the

1 Corresponding author: dijana_87@yahoo.com • https://orcid.org/0000-0001-6745-9623

eISSN 2620-0406

victim. Terms such as cyberbullying, doxing, trolling and swatting are increasingly entering professional and legal discourse, but also the everyday language of adolescents, parents, teachers and even judicial bodies. However, most of the research to date has focused primarily on the victims of these forms of violence, while the psychological profiles of the perpetrators themselves remain relatively under-researched.

The purpose of this study is to explore the psychological mechanisms and behaviour patterns of people who engage in digital aggression. It integrates social, cognitive, and behavioural psychology concepts including deindividuation (Zimbardo, 2007), moral disengagement (Bandura, 1999), and digital disinhibition (Suler, 2004). Additionally, the study presents a new concept to explain how perpetrators justify their involvement in online harassment. This new approach aims to clarify the moral reasoning processes that allow individuals to see their actions as acceptable or insignificant in digital spaces.

The work belongs to the field of criminal psychology, but it is also interdisciplinary, because it connects forensics, personality psychology, social psychology, and elements of digital ethics and law. It has potential application in prevention, education, legal system and psychosocial treatment of offenders, especially among adolescents and young adults. At a time when the boundaries between real and digital identities are becoming increasingly blurred, understanding the psychology of digital aggression is not just an academic issue, but also a matter of public health and safety.

UNDERSTANDING DIGITAL AGGRESSION

Contemporary society increasingly functions within a virtual environment, in which communication patterns and value systems have visibly changed, and violence in the digital space is becoming an almost daily experience for a large number of users of social networks, especially young people, who are also their most frequent users. Numerous studies, both in the domestic and international context, consistently indicate a high representation of those who at some point in their lives were exposed to violence on the Internet (Biswas et al., 2020; Aljaffer et al., 2021; Radoičić et al., 2024). Moreover, women constitute a particularly vulnerable and systematically under-protected group in the context of the digital environment (Powell & Henry, 2017; Arimatsu, 2019; Barter & Koulu, 2021; Nadim & Fladmoe, 2021).

Digital aggression is the intentional and repeated infliction of psychological harm on another person through electronic media, including social networks, forums, applications and other digital platforms (Kowalski et al., 2014; Mukred et al., 2024). In the interest of understanding this behaviour, it is necessary to consider not only the individual, but the digital context in which the aggression occurs. The digital environment creates algorithmic logic and online communities with norms specific to the digital space, which make particular forms of aggression normative and acceptable. Research shows that the algorithms of social networks push forward information that elicits strong emotions – anger, fear or hatred – as it leads to greater engagement with the user (Brady et al., 2017). In such an environment, aggressive behaviour, insults and humiliation can represent a pattern of behaviour that is rewarded socially and materially, also creating a culture of conflict. Young individuals who are continuing to develop their identity and sense of belonging can be especially vulnerable to this situation.

Anonymity is a major contributor to the enactment of digital aggression as it removes a sense of responsibility and enables a dissociation of online versus real-life identity (Lapidot-Lefler & Barak, 2012; Kim et al., 2023). In such a context, even people with developed self-control in offline environments can show aggressive tendencies. Aggression in digital space often takes place in front of an audience that, although they may not participate directly, contributes to the legitimization of violence and the strengthening of the aggressor through passive support or silence.

Among the different forms of digital aggression, cyberbullying and doxing stand out in particular (Fox, 2023). Cyberbullying refers to the systematic online harassment, threats, or exclusion of the victim, where attacks can be continuous, with a wide reach and a potentially permanent digital trail (Tokunaga, 2010). Doxing, on the other hand, involves the malicious disclosure and distribution of personal information without consent, with the aim of causing harm, intimidation, or public embarrassment (Citron, 2014; Douglas, 2016). The consequences of these procedures include anxiety, depressive symptoms, feelings of insecurity, and even serious psychological trauma in the victims (Veljković et al., 2021; Ali & Shahbuddin, 2022). Perpetrators, on the other hand, often exhibit low empathy, moral detachment and a high degree of anonymous aggression, which points to specific psychological patterns.

In certain online communities – such as forums, or social media groups – subcultures develop that institutionalize aggression, promote hate speech and rationalize violence against "others". These communities function through collective moral relativization, where attacking a targeted person or group is perceived as acceptable or even desirable behaviour. In this sense, the digital space no longer functions as a neutral communication platform, but as a mechanism of social control and stigmatization.

Digital aggression is a multifaceted phenomenon whose legal framework lags considerably behind its actual occurrence and diversity in practice (Dinić, 2022). While the Internet is a global network without borders, legal reactions to forms of violence in the digital realm – including cyberbullying and doxing – vary from country to country, which suggests the unevenness and fragmentation of legal norms. It is important for the purposes of more effective preventive action and protection of victims to adopt common standards while appreciating the situated cultural and social specificities that frame the manifestations of digital violence.

In the European Union in 2017, Germany was pioneering the way with legislation like "Network Enforcement Act" (Netzwerkdurchsetzungsgesetz, NetzDG) or so-called "Facebook Act" (Gesley, 2021), which mandates quick reactions from digital platforms to eliminate hate speech and threats, while France and Denmark specifically sanction doxing, or the publication and deliberation of personal data without consent (McCully, 2019). Sweden stands out by having imposed harsher penalties for online harassment while also acknowledging the psychological repercussions for victims (Citron, 2014). Within the United States digital aggression has yet to gain status as a separate crime but it is prosecuted through multiple legal channels, although case law in doxing has indicated an appetite for federal uniformity studies (Douglas, 2016).

As for prevention, some countries, such as Finland and the Netherlands, are introducing systemic educational programs aimed at developing digital literacy and ethics, including the concept of "digital empathy", which involves making young people aware of emotions

and the consequences of their behaviour in the digital space (Livingstone et al., 2019). In contrast, in many transition countries, including the majority of Balkan states, the prevention of digital violence is predominantly reactive, relying on individual initiatives and campaigns that follow incidents, while systemic education on digital rights and responsibilities is still not integrated into educational curricula (Jevtić, 2022; Bećirović-Alić & Saračević, 2022).

ONLINE ABUSER PROFILE

Recognizing and understanding the psychological characteristics of individuals who engage in forms of digital aggression, including cyberbullying and doxing, is a fundamental step for effective prevention and for creating strategic psychosocial interventions. Unlike traditional violent offenders, online perpetrators often act anonymously and from the "shadows", without an immediate physical threat, and this absence of immediacy allows the actor to more freely and without immediate fear of retaliation or sanctions act out on their aggressive impulses. This distance, reinforced by digital mediation effects, decreases the level of personal responsibility and encourages deindividuation, whereby individuals lose a sense of moral responsibility for their actions.

One of the most significant psychological predictors of a tendency towards online violence is elevated values on personality traits known as the Dark Triad – narcissism, Machiavellianism and psychopathy (Paulhus & Williams, 2002). These traits are characterized by manipulativeness, egocentrism, lack of empathy and emotional coldness. Narcissistic people seek attention and dominance, so they use social media as a platform to achieve status and power, regardless of means. Psychopathically oriented individuals show a tendency to callously inflict pain, which makes them a particularly dangerous group in the digital environment. Empirical research confirms that adolescents and youth with high scores on narcissistic dimensions more often post offensive content, exclude others from online groups, and even engage in blackmail by sharing private information (Ang & Goh, 2010). In addition, people with pronounced antisocial traits practice doxing more often, partly due to the dissociation between their own behaviour and its moral evaluation.

Impulsivity is also a noticeable risk factor for risky online behaviours (DeMarsico et al., 2022). Unlike face-to-face communication where there is delay or time to process information, online communication is often instantaneous and became entirely subject to impulsive responses – individuals communicating in this way often fail to think before acting. For example, earlier studies show that adolescents low in self-control and high in emotional reactivity are more likely to verbal aggression in online contexts (Bauman, 2015). Emotional dysregulation, which is the inability to regulate and appropriately express emotional states like anger, jealousy and frustration, further supports the potential of online aggression, as violence is often an acceptable release of negative emotionality that individuals face.

Another central aspect of the psychological profile of digital perpetrators is a low level of empathy, both cognitive (the ability to understand other people's emotions) and affective (emotional compassion). The absence of empathy enables moral distance and rationalization of aggressive behaviour, which is additionally intensified due to the absence of physical contact and immediate feedback in the digital environment.

The concepts of deindividualization (Zimbardo, 1969) and online disinhibition (Suler, 2004) further explain the psychological mechanisms behind digital aggression. Deindividualization reduces the sense of personal responsibility as individuals within an anonymous or mass online community lose their sense of individual identity. The effect of online disinhibition, benign on the one hand (expression of emotions, support), and toxic on the other (swear words, threats, humiliation, doxing), further enhances the expression of extreme and antisocial forms of behaviour. It is precisely in the toxic form of disinhibition that the psychological roots of phenomena such as trolling, doxing and online mobbing lie.

In addition, Bandura's (1999) theory of moral exclusion shows how perpetrators of aggressive acts in the digital realm engage in recycling strategies of moral dissociation-euphemizing ("this is just a joke"), dehumanizing ("that's not a real person, it's just a profile"), and diffusion of responsibility ("everyone is doing it") to explain their violent actions and expel any feelings of moral guilt.

This multi-dimensional approach clarifies the psychological processes that are at play in digital aggression and emphasizes that complex, multi-layered solutions are necessary that may include an increase in empathy, emotional regulation, and the enhancement of a sense of personal responsibility, in an online environment.

CROWD-CRUELTY COMFORT (CCC) CONCEPT

One of the central questions in the study of digital aggression psychology is how individuals are able to harm others via the internet without experiencing guilt, shame, or internal moral conflict. The answer lies in a psychological mechanism known as *moral disengagement* – a concept systematized by Albert Bandura (1999) to explain how individuals bypass internal ethical norms and social moral standards when engaging in aggressive acts.

Bandura's theory of moral exclusion points out that through certain cognitive strategies the internal moral compass can be "turned off" temporarily, which makes violent behaviour psychologically acceptable and rationalized. In the digital context, these mechanisms are additionally reinforced by the characteristics of the media – asynchrony, anonymity and the absence of immediate emotional feedback reduce empathic resonance and emotional distance towards the victim (Suler, 2004; Kowalski et al., 2014).

Mechanisms of moral exclusion often observed in perpetrators of online violence include:

- *Euphemizing behaviour*: Using humorous or neutral language to minimize aggression (Bandura, 1999) (e.g., "he was just kidding", "it was a meme, not a real threat");
- *Comparison with more severe forms of violence*: relativization of one's own behaviour through comparison with more serious acts (Bandura, 1999) ("It's nothing, it can be worse");
- *Dislocation of responsibility*: shifting responsibility to others or the collective (Bandura, 1999; Zimbardo, 2007) ("Everybody's doing it", "It's a trend");
- *Dehumanization of the victim*: perception of the victim as a less valuable being or unimportant identity (Staub, 2003) ("just a profile", "oversensitive person");
- *Blaming the victim*: attribution of guilt to the victim (Baumeister et al., 1994) ("She wanted attention", "She deserved criticism").

These patterns allow aggressors to inflict serious emotional, reputational, and psychological damage while maintaining a positive or neutral moral view of themselves.

Especially in the digital context, ironic and cynical communication often serves as a mask for aggression. Doxing, online lynchings, offensive comments and humiliation are often presented as "jokes" or "satire", which serves a dual purpose: reducing the perception of the seriousness of the violence and making it difficult to sanction the perpetrators socially or legally (Shifman, 2013). This kind of humour in the function of moral exclusion reflects cognitive dissociation – a process in which the victim is reduced to an object of entertainment or a means of expressing power (Phillips, 2015).

Social dynamics in online communities further reinforce moral disengagement. The phenomenon of the "digital crowd" (or online crowding) reduces individual responsibility due to the diffusion of accountability (Latané & Darley, 1970; Zimbardo, 2007). In instances of mass dissemination of offensive content, users who like, share, or comment during coordinated digital attacks often experience a diminished sense of personal responsibility. This fosters collective rationalization and hinders intervention (Salmivalli, 2010).

In this context, moral exclusion is not only an individual psychological process, but also a cultural phenomenon, replicated through the norms and practices of Internet communities. Individuals are able to maintain destructive behaviours through mechanisms that support their perception of moral correctness. In the dominant discourses on digital violence, the focus is usually on the primary actors – people who directly send threats, publish sensitive data, create offensive content or initiate coordinated attacks (hunts) against individuals. However, secondary actors, known as hidden supporters or shadow supporters, who, although they do not formally initiate violence, give legitimacy with their behaviour, spread aggressive messages and increase their effect, have psychological and social significance.

The fundamental difference between active perpetrators and covert supporters is not only reflected in the degree of immediacy of their actions, but also in their psychological motivation, perception of responsibility, way of engagement and mechanisms of moral dissociation. Perpetrators are typically aware of their aggressive intentions and consciously use violence as a means of exerting control, venting frustration, or enhancing social status. In contrast, shadow supporters often see themselves as neutral observers, commentators, or members of the online audience – despite their actions indirectly contributing to the spread and normalization of violence.

The psychological profile of shadow supporters is characterized by a significant perceptual distance from the aggression itself, which allows them to minimize the feeling of personal responsibility. For example, they will not publish someone else's private data themselves, but will support such content by liking or sharing, further spreading the damage. They often justify their actions through ironic comments, wit or passive statements such as: "I just reposted", "I didn't write that, I just commented". This ethical and emotional "grey zone" makes covert supporters a key factor in maintaining and escalating digital aggression.

While the perpetrator acts directly and visibly, with the aim of destruction and domination, the shadow supporter acts from the sidelines, but without their support and active involvement the effect of the aggression would be significantly weakened. These supporters most often come from circles of friends, acquaintances, followers or other members of the community who, out of fear, conformity or latent sadistic tendencies, contribute to maintaining a hostile atmosphere, although they never take on the role of initiator.

Psychological phenomena associated with this behaviour include conformity, diffusion of responsibility and moral dissociation – mechanisms that allow individuals to participate in violence without internal conflict, while maintaining a perception of themselves as "normal", "neutral" or even "moral" persons. For this reason, covert supporters are extremely important for understanding the dynamics of the spread, strengthening and maintenance of digital aggression – a process that takes place silently, gradually and extremely effectively in the online environment.

Based on theoretical analysis and current literature, a comprehensive classification framework for digital actors involved in online aggression is proposed. This framework incorporates dimensions such as engagement level, behaviour type, motivation, and moral self-perception (Bandura, 1999; Suler, 2004). Its application in education, psychology, and forensics allows for more precise identification of aggression dynamics and the development of targeted prevention and intervention strategies (Kowalski et al., 2014).

To more precisely describe these specific forms of moral disengagement in the digital context, the CCC concept is introduced. CCC represents a psychological process in which digital aggressors reinterpret their harmful behaviour – such as doxing, sharing offensive content, or spreading defamation – as morally justified. They construct a narrative of their own moral correctness, often framing their actions as altruistic or protective of the community, without realistically considering the consequences for others.

Unlike classical moral disengagement, CCC involves not just the suppression of guilt but the *active construction* of a moral identity in which the aggressor sees themselves as ethically superior. The victim is reframed as guilty, manipulative, or dangerous – someone who deserves punishment (Fiske & Rai, 2015). In other words, CCC is a dynamic process of moral self-defence and ethical rationalization.

Specific defence mechanisms that characterize CCC include:

- Rationalization: framing violence as criticism, public interest, or protection (Freud, 1936; Bandura, 1999);
- Moral dissociation: suspending internal moral norms while affirming one's moral self-image (Bandura, 1999);
- Diffusion of responsibility: legitimizing violence through collective behaviour ("Everyone is doing it") (Zimbardo, 2007);
- Projection and victim-blaming: attributing malicious intent or fault to the victim as a form of self-defence (Baumeister et al., 1994).

Specificities of the digital context. Digital media provide specific characteristics that facilitate the development and maintenance of CCC:

1) Asynchrony and physical distance – enable emotional distance and reduce empathic resonance (Suler, 2004);
2) Fragmentation of identity – creation of online "masks" that protect from the feeling of authentic responsibility (Turkle, 2011);
3) Culture of moral signalling – the need to demonstrate moral correctness, often instrumentalized and superficial (Bicchieri, 2006);
4) A collective culture of "online purity" – where moral discourse is used as a tool of positioning rather than genuine ethical reflection (Marwick & Boyd, 2011).

In such conditions, labelling others as "toxic", "manipulative" or "problematic" often serves more to protect personal or group status than to provide real moral intervention, which further reproduces the cycle of digital aggression.

Understanding moral exclusion and digital moral self-justification is essential for analysing and intervening in the phenomena of online violence and digital aggression. These concepts illuminate the internal psychological mechanisms that allow individuals to continue aggressive behaviour without guilt, while maintaining a positive moral identity. The role of technology and social norms further reinforces these processes, which requires a multidisciplinary approach to prevention and education about healthy digital communication.

Phased Processes of CCC Concept

In terms of conceptualising CCC temporally, we could offer a phased model of *how it develops within virtual communication systems* by structuring the model in phases:

1) The first phase of CCC is the *perception of moral threat*, where a user becomes aware of another user, who is perceived to be behaving immorally or unacceptably.
2) In the second phase, *reaction* occurs through various types of digital behaviour – offensive comments, public exposure (doxing), symbolic rejecting (e.g., liking unsafe content that includes a representation of the target).
3) The third phase involves *feedback*, where the digital community subsequently reacts to the signaller's behaviour including the experience of the target of the initial behaviour (the original user) or the broader social context, which can be interpreted as either positive (e.g., supportive) or negative (e.g., critiquing the signaller's action).
4) The fourth phase is *cognitive dissonance*, where there was a harmful or immoral action in the view of the signaller and their perception of themselves did not match the environment/situation (e.g., "Maybe I went too far after all").
5) The final stage is *CCC activation*. This dissonance is reduced through reinterpretation of one's own motivation (e.g., "I just wanted to help", "I care about society").
6) Finally, in the sixth stage, *narrative stabilization* occurs, where the signaller reaffirms their own moral position and shifts the focus to the problematic nature of the other person's behaviour (e.g., "I'm not the problem, they are").

This six-stage model provides a theoretical framework for analysing the psychosocial mechanisms behind CCC, and allows the researcher to more precisely identify the patterns and logic of this form of online behaviour.

In order to gain a deeper understanding of the complexity of the phenomenon of CCC concept, a conceptual differentiation of its manifestations is proposed through the identification of three preliminary subtypes: reactive, collective, and strategic self-justification. This classification enables a more precise mapping of different motives, dynamics and contexts in which CCC occurs, and opens up space for further theoretical elaboration and empirical operationalization of the term.

Reactive self-justification refers to the impulsive, affectively coloured reaction of an individual immediately after their behaviour in the digital space is called into question. This form is characterized by speed, emotional intensity and the absence of reflective distance

– often manifested through statements like "I was only telling the truth!" or "I defended myself!", without a deeper rationalization.

Collective CCC is formed within group digital environments, where narratives of justification are shaped, confirmed, and reinforced through interaction with community members (e.g., forums, social networks, comment sections). In this form of CCC, individual responsibility is diluted and legitimacy is derived from belonging to a majority discourse or shared moral position.

Strategic self-justification, unlike the previous two, represents a planned and thoughtfully constructed narrative by which an individual tries to present himself as morally consistent, rational and socially acceptable. This form is most often used in the context of preserving digital identity, reputation, or status, and may involve sophisticated rhetorical strategies, selective presentation of information, or appeals to universal moral values.

The proposed concept distinguishes five basic types of actors, distributed along a continuum from direct perpetrators to passive accomplices, thus illuminating different functions and responsibilities within the network of online aggression:

1. Initiator (Perpetrator of Aggression)

The initiator is the main agent of aggressive action, who actively carries out violence by insulting, humiliating, doxing, spreading false information, threats or organizing coordinated campaigns (hunts). The psychological profile of these actors often includes high impulsivity, low empathy, and pronounced traits of the "dark triad" – narcissism, Machiavellianism, and psychopathy (Paulhus & Williams, 2002; Jones & Paulhus, 2014). Moral distance towards the consequences of their actions enables them to rationalize or completely deny guilt (Bandura, 1999).

2. Executor (Functional Accomplice)

Executors do not initiate violence, but actively participate in its spread, sharing offensive content, generating additional materials or distributing private information. Their motivation may be related to group pressure, loyalty or personal gain (Festinger, 1954; Cialdini & Goldstein, 2004). They often show perceptual and emotional distance towards victims, which facilitates dehumanization and reduces empathy (Haslam, 2006).

3. Shadow Supporter

This category includes users who are not formally directly involved in violence, but through their passive or indirect behaviour – such as liking, sharing, humorous comments or remaining silent at key moments – maintain and multiply aggressive content. They often perceive themselves as neutral or disengaged subjects, which enables moral dissociation and minimization of the sense of responsibility (Suler, 2004; Bandura, 1999). Their contribution has an exponential effect on the spread of violence in digital communities (Kowalski et al., 2014).

4. Observer (Passive Actor)

Observers are witnesses of violent events who do not react in any way. Their inactivity stems from fear, indifference or a feeling of powerlessness (Latané & Darley, 1970). Although passive, their lack of reaction implicitly tolerates and normalizes aggressive behav-

iour, which can worsen the situation (Bandura, 1999). This role is particularly common among children and adolescents, emphasizing the need for education about digital courage and active ethical responsibility.

5. Intervenor (Victim's Advocate)

Intervenors actively oppose violence, report harmful content, provide support to victims and educate the community (Patchin & Hinduja, 2010). This type of actor, although rarer, is key to breaking the cycle of violence. Psychologically, they are characterized by high emotional empathy, a strong sense of justice, and a low need for social approval (Batson et al., 2002).

Comparing CCC to Other Forms of Cognitive Distortion

For a deeper theoretical understanding of the CCC concept, it is useful to compare this phenomenon with other known forms of cognitive distortions that occur in social and moral behaviour. Although CCC shares certain features with mechanisms such as moral exclusion, cognitive dissonance, and rationalization, it differs in the specific way it constructs and stabilizes a moral self-image within digital environments.

Table 1. *A Comparison of the CCC Concept with Other Cognitive Distortions*

	Key Characteristic	Key Differences from CCC
Moral exclusion	Neglecting or suspending moral responsibility towards others	Unlike moral exclusion, which eliminates moral obligation, CCC actively constructs a positive moral identity and justifies behaviour as socially useful.
Cognitive dissonance	Internal psychological conflict due to a discrepancy between beliefs and behaviour	CCC acts as a mechanism to eliminate dissonance by reinterpreting motivations and creating a coherent moral narrative.
Rationalization	Subsequent logical justification of behaviour that would otherwise cause discomfort	Although CCC also includes elements of rationalization, it is additionally characterized by emotional identification with one's own moral status and the desire to maintain a positive public (and self-perceptive) identity.

This comparative analysis shows that CCC, although rooted in a wider spectrum of psychological defence mechanisms, represents a special form of cognitive-emotional processing in the digital environment. The key distinctive feature of CCC is its function to not only rationalize behaviour, but also to present it as morally justified, often with an implicit or explicit emotional need to confirm one's own moral value in the eyes of a digital audience.

This differentiation is not only theoretically valuable, but also provides a basis for more precise operationalization of the CCC in future research, as well as for the development of criteria that can distinguish this phenomenon from related, but functionally different forms of moral cognition and self-assessment.

CONCLUSION
APPLICATIONS OF CCC IN EDUCATION, PREVENTION, AND PSYCHOSOCIAL INTERVENTION

CCC is an innovative concept in psychology and education that explains how authority figures – such as teachers, psychologists, or therapists – can recognize and expose the internal structures of self-justification that students or perpetrators use in digital violence. Understanding CCC enables the development of target workshops for critical reflection of online behaviours, supports clients in distinguishing the real moral position from the constructed narrative position, and encourages work on authenticity, empathy and self-compassion. In addition to practical application in education, the CCC concept provides a framework for building a psychometric instrument that can be used to measure moral self-justification in an online context – through items such as: "My posts serve to protect people, even if they hurt someone", or "The same rules do not apply in the virtual world as in reality". This instrument can serve as a basis for campaigns that avoid defensiveness in the audience and indirectly deconstruct false moral narratives, as well as for the creation of legislative frameworks that recognize the hidden aggression behind morally coloured expressions.

In light of the increasing prevalence of digital aggression and the harmful consequences it causes – both for victims and for society as a whole – it is necessary to develop systematic preventive and intervention mechanisms that include educational, psychological, legal and technological sectors. Prevention must go beyond passive warning about the "dangers of the Internet" and include risk assessment, development of empathy, digital competence and sense of responsibility, and cooperation with platforms and legislative bodies.

By combining theoretical knowledge about moral exclusion and CCC concept with systematic preventive and intervention measures, it is possible to develop a comprehensive and multidisciplinary approach to combat aggression in the digital space. At the moment when internet communication becomes a central aspect of everyday life, understanding the psychology of digital actors – their motivations and self-rationalization – is essential for the creation of effective education, policy and practice that protects the individual and society.

REFERENCES

Ali, S. I., & Shahbuddin, N. B. (2022). The relationship between cyberbullying and mental health among university students. *Sustainability*, *14*(11), 6881. https://doi.org/10.3390/su14116881

Aljaffer, M., Alshehri, K., Almutairi, M., Aljumaiah, A., Alfraiji, A., Hakami, M., AlDossary, M., & Irfan, T. (2021). Cyberbullying among young Saudi online gamers and its re-

lation to depression. *Journal of Nature and Science of Medicine*, *4*(2), 142–147. https://doi.org/10.4103/jnsm.jnsm_78_20

Ang, R. P., & Goh, D. H. (2010). Cyberbullying among adolescents: The role of affective and cognitive empathy, and gender. *Child Psychiatry and Human Development*, *41*(4), 387–397. https://doi.org/10.1007/s10578-010-0176-3

Arimatsu, L. (2019). Silencing women in the digital age. *Cambridge International Law Journal*, *8*(2), 187–217. http://dx.doi.org/10.4337/cilj.2019.02.02

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209. https://doi.org/10.1207/s15327957pspr0303_3

Barter, C., & Koulu, S. (2021). Digital technologies and gender-based violence – mechanisms for oppression, activism and recovery. *Journal of Gender-Based Violence*, *5*(3), 367–375. https://doi.org/10.1332/239868021X16315286472556

Batson, C. D., Ahmad, N., Lishner, D. A., & Tsang, J.-A. (2002). Empathy and altruism. In C. R. Snyder, & S. J. Lopez (Eds.), *Handbook of positive psychology* (pp. 485–498). Oxford University Press.

Bauman, S. (2015). *Cyberbullying: What counselors need to know.* American Counseling Association.

Baumeister, R. F., Stillwell, A. M., & Heatherton, T. F. (1994). Guilt: An interpersonal approach. *Psychological Bulletin*, *115*(2), 243–267. https://doi.org/10.1037/0033-2909.115.2.243

Bećirović-Alić, M., & Saračević, M. (2022). Violence in cyberspace and possible prevention. *Science and Research Journal*, *5*(2), 82–86. http://dx.doi.org/10.18421/SAR52-03

Bicchieri, C. (2006). *The grammar of society: The nature and dynamics of social norms*. Cambridge University Press.

Biswas, T., Scott, J. G., Munir, K., Thomas, H. J., Huda, M. M., Hasan, M. M., de Vries T. D., Baxter, J., & Mamun A. A. (2020). Global variation in the prevalence of bullying victimisation amongst adolescents: Role of peer and parental supports. *EClinicalMedicine*, 20, 100276.

Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. *PNAS Proceedings of the National Academy of Sciences of the United States of America*, *114*(28), 7313–7318. https://doi.org/10.1073/pnas.1618923114

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*, 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Citron, D. K. (2014). *Hate crimes in cyberspace.* Harvard University Press.

DeMarsico, D., Bounoua, N., Miglin, R., & Sadeh, N. (2022). Aggression in the digital era: Assessing the validity of the cyber motivations for aggression and deviance scale. *Assessment*, *29*(4), 764–781. https://doi.org/10.1177/1073191121990088

Dinić, B. (2022). *Digitalno nasilje.* Filozofski fakultet Univerziteta u Novom Sadu.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, *18*(3), 199–210. https://doi.org/10.1007/s10676-016-9406-0

Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, *7*(2), 117–140. https://doi.org/10.1177/001872675400700202

Fiske, A. P, & Rai, T. S. (2015). *Virtuous violence: Hurting and killing to create, sustain, end, and honor social relationships.* Cambridge University Press.

Fox, J. (2023). Online social aggression: Harassment and discrimination. In R. L. Nabi, & J. Gall Myrick (Eds.), *Emotions in the digital world: Exploring affective experience and expression in online interactions* (pp. 193–214). Oxford University Press. https://doi.org/10.1093/oso/9780197520536.003.0011

Freud, A. (1936). The ego and the mechanisms of defense. In: *The writings of Anna Freud* (Vol. 2) (pp. 3–191). International Universities Press.

Gesley, J. (2021). *Germany: Network Enforcement Act amended to better fight online hate speech.* Library of Congress Website. Retrieved from https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/.

Haslam, N. (2006). Dehumanization: An integrative review. *Personality and Social Psychology Review*, *10*(3), 252–264. https://doi.org/10.1207/s15327957pspr1003_4

Jevtić, R. B. (2022). Digitalno nasilje među učenicima srednjih škola. *Zbornik radova Pedagoškog fakulteta, Užice*, *24*, 45–62. https://doi.org/10.5937/ZRPFU2224045J

Jones, D. N., & Paulhus, D. L. (2014). Introducing the Short Dark Triad (SD3): A brief measure of dark personality traits. *Assessment*, *21*(1), 28–41. https://doi.org/10.1177/1073191113514105

Kim, M., Ellithorpe, M., & Burt, S. A. (2023). Anonymity and its role in digital aggression: A systematic review. *Aggression and Violent Behavior*, 72, 101856. https://doi.org/10.1016/j.avb.2023.101856

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

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, *28*(2), 434–443. https://doi.org/10.1016/j.chb.2011.10.014

Latané, B., & Darley, J. (1970). *The unresponsive bystander: Why doesn't he help?* Appleton-Century Crofts.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review.* London School of Economics and Political Science.

Marwick, A., & Boyd, D. (2011). To see and be seen: Celebrity practice on twitter. *Convergence*, *17*(2), 139–158. https://doi.org/10.1177/1354856510394539

McCully, J. (2019). *Legal responses to online harassment and abuse of journalists: Perspectives from Finland, France and Ireland*. Organization for Security and Cooperation in Europe. https://www.osce.org/files/f/documents/1/6/413552.pdf

Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei, A., Sadiq, A. S., & Al-Othmani, A. (2024). The roots of digital aggression: exploring cyber-violence through a systematic literature review. *International Journal of Information Management Data Insights*, *4*(2), 100281. https://doi.org/10.1016/j.jjimei.2024.100281

Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, *39*(2), 245–258. https://doi.org/10.1177/0894439319865518

Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of School Health*, *80*(12), 614–621. https://doi.org/10.1111/j.1746-1561.2010.00548.x

Paulhus, D. L., & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*(6), 556–563. https://doi.org/10.1016/S0092-6566(02)00505-6

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. The MIT Press.

Powell, A., & Henry, N. (2017). *Sexual violence in digital age*. Palgrave Macmillan. https://doi.org/10.1057/978-1-137-58047-4

Radoičić, D., Stojić, V., Zdravković, N., Stojanović, S., Ilić, V., & Lukić, D. (2024). Razumevanje uticaja digitalne tehnologije na mentalno zdravlje i nasilničko ponašanje adolescenata. *PONS – medicinski časopis*, *21*(1), 8–13. https://doi.org/10.5937/pomc21-50597

Salmivalli, C. (2010). Bullying and the peer group: A review. *Aggression and Violent Behavior*, *15*(2), 112–120. https://doi.org/10.1016/j.avb.2009.08.007

Shifman, L. (2013). *Memes in digital culture*. MIT Press.

Staub, E. (2003). *The psychology of good and evil: Why children, adults, and groups help and harm others.* Cambridge University Press. https://doi.org/10.1017/CBO9780511615795

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*(3), 277–287. https://doi.org/10.1016/j.chb.2009.11.014

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

Veljković, B., Mihajlović, M., Dukić, S., & Despotović, M. (2021). Nasilje na društvenim mrežama. *PONS – medicinski časopis*, *18*(2), 84–91. https://doi.org/10.5937/pomc18-36747

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In W. J. Arnold, & D. Levine (Eds.), *Nebraska symposium on motivation* (Vol. 17) (pp. 237–307). University of Nebraska Press.

Zimbardo, P. (2007). *The Lucifer effect: Understanding how good people turn evil.* Random House.