Registered in Germany Europa Revue Journal
ISSN: 1862-6564 Vol. 6 No. 5 (2026) Published May 31, 2026

PHILOSOPHICAL FOUNDATIONS OF DEVELOPING YOUTH DIGITAL RESILIENCE AGAINST HYBRID THREATS

Baratov Jasur Ulmasovich
Independent Researcher at Fergana State University (Fardu)
Orcid: 0009000086481711
baratovjasur344@gmailcom

Abstract

The rapid expansion of digital communication has fundamentally transformed the ways in which young people acquire information, construct social identities, form opinions, and participate in public life. At the same time, the digital environment has become an important domain in which hybrid threats can operate through combinations of information manipulation, cyber operations, psychological influence, coordinated inauthentic behaviour, and other non-military instruments. This article examines the philosophical foundations of developing young people's digital resilience against hybrid threats. The study approaches digital resilience not merely as a technical ability to protect personal data or devices, but as a multidimensional social and philosophical capacity involving critical thinking, epistemic responsibility, ethical judgement, media and information literacy, and the ability to preserve individual autonomy in a rapidly changing information environment. The article argues that effective resilience should not be reduced to censorship or simple rejection of unfamiliar information. Rather, it should be based on the development of autonomous judgement, responsible digital citizenship, critical reflection, and the ability to distinguish evidence from manipulation. Particular attention is given to the role of education, social institutions, digital platforms, families, universities, and public policy in creating an environment in which young people can recognise and resist manipulative information without losing their openness to legitimate pluralism. The article concludes that youth digital resilience should be understood as a component of contemporary social security and as an important condition for maintaining individual autonomy, social trust, and the integrity of the public information environment.

Keywords

hybrid threats, digital resilience, youth, social consciousness, digital environment, media literacy, misinformation, critical thinking, information security, philosophy of education.

Introduction

Digitalisation has become one of the defining characteristics of contemporary social development. The Internet, social media, mobile applications, online communities and artificial intelligence have created new opportunities for education, communication, creativity and civic participation. For younger generations in particular, digital communication is not simply an additional instrument of interaction; it has become an important environment in which social experience is acquired and interpreted. Recent OECD research describes social media as increasingly central to the ways in which young people communicate and consume information.[1] This transformation creates significant opportunities, but it also produces new forms of vulnerability.

One of the most important challenges is the emergence and development of hybrid threats in the digital environment. Contemporary approaches generally understand hybrid threats as coordinated harmful activities that may combine different instruments, including information manipulation, cyberattacks, economic pressure, covert influence and other means, often while remaining below the threshold of formally declared warfare.[2] The European Centre of Excellence for Countering Hybrid Threats and the European Commission have emphasised that hybrid activities can exploit vulnerabilities across several domains and use different tools in combination.[3]

The significance of this problem for young people is associated not only with the amount of time they spend online, but also with the developmental role of information in the formation of their worldview. Digital content can affect perceptions of social reality, trust in institutions, attitudes toward other groups, interpretations of historical events, cultural values and personal identity. Consequently, the problem of hybrid threats should not be examined exclusively through the lens of cybersecurity. It also requires a social-philosophical analysis of human autonomy, truth, responsibility, freedom, identity and social trust.

The central research problem of this article is therefore the following: what philosophical principles should underpin the development of young people's digital resilience in conditions where information manipulation and other hybrid threats increasingly operate through digital communication environments?

The article proceeds from the assumption that digital resilience is not synonymous with technological protection. A young person may possess considerable technical knowledge while remaining vulnerable to manipulation if he or she lacks the ability to critically evaluate information, recognise emotional pressure, examine sources and reflect on personal cognitive biases. Thus, resilience must combine technological, cognitive, ethical and social dimensions.

Hybrid Threats as a New Dimension of Social Reality

The concept of hybrid threats has evolved in response to changes in the security environment. The contemporary conceptual model developed by the European Commission's Joint Research Centre and the Hybrid CoE analyses hybrid threats through several interconnected components: actors, strategic objectives, domains, tools and phases of activity.[3] This approach is important because it demonstrates that hybrid threats cannot be reduced to one particular technology or method.

Information manipulation is particularly relevant to the digital environment. Social networks enable information to circulate rapidly between individuals and communities. A misleading message can be reproduced thousands of times without its original context, while emotionally provocative content may attract greater attention than carefully verified information. The resulting problem is therefore not simply whether a particular statement is true or false. It is also concerned with the social conditions under which people decide what to believe, share and emotionally respond to.

Wardle and Derakhshan distinguish between misinformation, disinformation and malinformation as different forms of information disorder.[4] This conceptual distinction is useful because not every false statement is necessarily the product of deliberate manipulation. Misinformation can be shared without an intention to cause harm, whereas disinformation involves deliberately deceptive or misleading content. Such distinctions are particularly important when developing educational responses

because effective digital resilience requires individuals to understand not only the content of information but also its context, source, intention and potential consequences.

From a philosophical perspective, hybrid influence raises a fundamental question concerning the autonomy of the individual. Classical conceptions of autonomy assume that a person is capable of making considered judgements rather than simply responding to external pressure. In the digital environment, however, decisions can be influenced by algorithms, social approval mechanisms, emotionally charged content and repeated exposure to particular narratives. Therefore, the protection of autonomy requires more than legal rights or technical security; it requires intellectual and ethical capacities that enable individuals to reflect upon the influences acting upon them.

Digital Resilience as a Philosophical Category

The concept of resilience is commonly associated with the ability of individuals and societies to withstand disturbances and recover while maintaining essential functions. In the context of hybrid threats, resilience is increasingly understood as a whole-of-society task rather than the responsibility of security institutions alone.[5]

Digital resilience can consequently be defined as the ability of individuals and communities to maintain autonomous, responsible and informed behaviour in the face of misleading, manipulative, hostile or disruptive digital influences.

Such a definition contains several philosophical dimensions.

First, there is an **epistemic dimension**. Individuals need the ability to distinguish knowledge from assumption, evidence from assertion, and verified information from unsupported claims. This is particularly significant because digital environments contain an unprecedented volume of information. OECD research has identified media literacy as an important component of policies designed to reduce risks associated with false and misleading digital content.[6]

Second, there is an **ethical dimension**. Digital resilience does not end with recognising misinformation. Individuals must also consider whether sharing uncertain information could harm another person, intensify social hostility or contribute to collective panic. Thus, responsible digital behaviour involves not only the question "Is this information true?" but also "What are the consequences of my actions?"

Third, there is an **autonomy dimension**. Resilience requires the ability to pause, reflect and make an independent judgement. A person who automatically shares information because it generates anger, fear or excitement may become an unwitting participant in an influence campaign. Consequently, the capacity for self-reflection becomes an essential element of digital security.

Fourth, there is a **social dimension**. Trust is a fundamental resource of social life. Persistent manipulation can weaken trust between citizens, institutions and social groups. The European Commission's conceptual work on hybrid threats highlights the potential of such activities to undermine public trust, deepen polarisation and affect decision-making.[3] Digital resilience should therefore contribute to the preservation of constructive social relations rather than simply encouraging defensive individualism.

Youth Social Consciousness in the Digital Environment

Young people occupy a particularly significant position in the digital information environment. They are active consumers and producers of online content and frequently participate in communities whose boundaries are not determined by geographical location. The digital environment consequently contributes to the formation of social consciousness.

Social consciousness can be understood as the system of ideas, values, beliefs, attitudes and perceptions through which individuals and groups interpret social reality. In the digital age, this consciousness is increasingly shaped by interactions between personal experience, institutional communication, peer networks, online influencers, news organisations and algorithmically organised content.

This does not mean that digital technologies mechanically determine young people's beliefs. Such a deterministic approach would underestimate individual agency. Rather, digital platforms create environments that structure the visibility and circulation of information. The individual remains capable of critical judgement, but the conditions under which that judgement takes place have changed.

Research on misinformation provides an important insight here. Pennycook and colleagues found that people's willingness to share false content can partly reflect insufficient attention to accuracy at the moment of sharing.[7] Their experimental

findings suggest that prompting users to consider accuracy can improve the quality of subsequent sharing decisions. From a philosophical perspective, this indicates that small acts of reflection can have broader social consequences.

Similarly, research by Roozenbeek and van der Linden demonstrated that educational interventions designed around common misinformation techniques can increase psychological resistance to misleading content.[8] Their work supports the broader proposition that resilience can be cultivated rather than treated as an innate personal characteristic.

Therefore, the development of youth digital resilience should focus on strengthening the capacity for reflection rather than simply providing lists of prohibited or unreliable sources.

Media and Information Literacy as the Foundation of Digital Resilience

Media and information literacy represents one of the most important practical expressions of digital resilience. UNESCO defines media and information literacy in terms of the capacities needed to access, analyse, evaluate and create content critically and responsibly.[9] This understanding is broader than conventional computer literacy.

Technical competence answers the question of how to use a technology. Media and information literacy additionally addresses how to understand and evaluate what technology communicates.

For young people, such literacy should include at least five interconnected abilities:

1. Source evaluation. Young people should learn to examine who produced information, what evidence is provided, when it was published and whether independent sources confirm the claim.

2. Contextual analysis. A genuine photograph, quotation or statistic can still be misleading if it is presented without its original context.

3. Recognition of manipulation techniques. Users should be familiar with emotional baiting, false dilemmas, impersonation, fabricated evidence, conspiracy narratives and other common techniques of information manipulation.

4. Reflective sharing. Before reposting information, individuals should consider whether it is sufficiently verified and whether its circulation may cause unnecessary harm.

5. Understanding of algorithms and artificial intelligence. Young people increasingly need to understand that digital content may be selected, recommended, generated or amplified through automated systems.

The relevance of these competencies has increased with the development of generative artificial intelligence. UNESCO has emphasised the growing need for AI literacy as generative AI becomes integrated into education, culture and everyday digital activity.[9] The European Commission's updated 2026 guidelines for educators likewise address disinformation, generative AI, social media platforms, influencers and prebunking strategies.[10]

Thus, contemporary digital resilience should include not only media literacy but also a foundational understanding of AI-generated and algorithmically mediated information.

Critical Thinking and the Preservation of Individual Autonomy

Critical thinking should not be understood as the automatic rejection of information. Such an approach could produce another form of cognitive vulnerability: the assumption that everything unfamiliar is false or hostile. Genuine critical thinking requires openness combined with evidence-based judgement.

The philosophical foundation of critical thinking is therefore intellectual autonomy. An autonomous individual does not simply accept or reject information according to group identity. Instead, he or she asks questions about evidence, reasoning, context and consequences.

This principle is particularly important in the context of hybrid threats because manipulation frequently exploits pre-existing social divisions. If individuals are trained only to distrust external information, they may become increasingly dependent on closed communities that confirm their existing beliefs. Such a situation can intensify polarisation rather than strengthen resilience.

A more productive model is reflective scepticism. Reflective scepticism does not assume that every claim is false; it temporarily suspends judgement until sufficient evidence becomes available. This approach allows individuals to remain open to legitimate disagreement while reducing susceptibility to manipulation.

The importance of cognitive reflection is also supported by empirical research. Pennycook and colleagues found relationships between cognitive reflection and the ability to distinguish true from false content in social-media contexts.[7] Such findings provide empirical support for a philosophical proposition: the capacity to pause before accepting or sharing information is a socially valuable intellectual habit.

Ethical Responsibility and Digital Citizenship

Digital resilience cannot be separated from ethical responsibility. Every user of a digital platform is not only a consumer but potentially also a distributor of information. Consequently, individuals participate in the construction of the information environment.

Digital citizenship should therefore be based on several ethical principles: respect for human dignity, responsibility for one's communication, rejection of deliberate deception, respect for privacy, tolerance of legitimate disagreement and willingness to correct mistakes.

This perspective is particularly important for young people because online behaviour can have consequences beyond the immediate digital interaction. A false accusation, manipulated image or inflammatory message may affect an individual's reputation, psychological well-being or social relationships.

An ethical approach also requires recognising the difference between legitimate disagreement and manipulation. A person may hold an unpopular opinion without being a participant in a hybrid influence campaign. Therefore, resilience education should not teach young people to classify disagreement itself as a threat. Instead, it should teach them to examine the methods by which claims are constructed and circulated.

Such an approach protects both security and freedom. Excessive control over information may weaken critical autonomy, while complete indifference to manipulation

may expose individuals and societies to significant risks. The philosophical challenge is therefore to establish a balance between freedom, responsibility and security.

Institutional Foundations of Youth Digital Resilience

The development of digital resilience cannot be delegated to young people alone. It requires cooperation among educational institutions, families, civil society, technology companies, researchers and public authorities.

Schools and universities should integrate media and information literacy into existing curricula rather than treating it as a narrow technical subject. Students should be encouraged to analyse real examples, compare sources, identify manipulative techniques and reflect on ethical consequences.

Teachers themselves require continuing professional development. The European Commission's 2026 guidelines explicitly emphasise the role of educators in strengthening students' digital literacy and addressing contemporary forms of disinformation, including AI-generated content and social-media influence.[10]

Families also have an important role. Parents can support resilience by creating an environment in which young people feel comfortable questioning information and discussing controversial content rather than simply receiving prohibitions.

Digital platforms have responsibilities as well. Transparency regarding recommendation systems, effective mechanisms for reporting harmful manipulation, and accessible information about synthetic or altered content can contribute to a healthier information environment. However, technological interventions should be accompanied by education because no platform-level solution can replace individual judgement entirely.

The Uzbek context is also relevant. UNESCO reported in 2025 that media and information literacy has increasingly been recognised in Uzbekistan as an important component of building a resilient and informed society, with stakeholders from government institutions, universities, media, civil society and academia participating in discussions on strengthening media competence.[11] This indicates the relevance of a coordinated, society-wide approach.

A Philosophical Model for Youth Digital Resilience

Based on the preceding analysis, youth digital resilience can be conceptualised as a system consisting of five mutually reinforcing components.

The first component is epistemic resilience. It is the capacity to evaluate evidence, distinguish fact from opinion and recognise uncertainty.

The second is cognitive resilience. It involves reflective thinking, resistance to impulsive reactions and awareness of one's own cognitive biases.

The third is ethical resilience. It represents the ability to recognise the social consequences of one's digital behaviour and act responsibly.

The fourth is social resilience. It involves maintaining constructive communication, resisting polarisation and preserving social trust while accepting legitimate diversity of opinion.

The fifth is technological resilience. It includes basic cybersecurity, understanding of algorithms, awareness of AI-generated content and safe use of digital platforms.

These dimensions should not be developed independently. Technical security without critical thinking may protect a device while leaving the individual vulnerable to manipulation. Critical thinking without ethical responsibility may produce sophisticated but socially harmful communication. Ethical awareness without technological competence may be insufficient in an environment of increasingly complex digital threats.

The philosophical objective is therefore the development of a digitally autonomous person: an individual who can use digital technologies while retaining the ability to think, evaluate, choose and act responsibly.

Conclusion

Hybrid threats in the digital environment represent not only a technological or security challenge but also a challenge to human autonomy, social trust and the formation of social consciousness. Young people are particularly significant in this context because digital communication constitutes an important part of their educational, cultural and social experience.

The analysis demonstrates that youth digital resilience should not be reduced to technical cybersecurity or the passive avoidance of allegedly dangerous information. Its

deeper foundation lies in the development of autonomous judgement, critical thinking, epistemic responsibility, ethical awareness and media and information literacy.

The philosophical foundations of digital resilience can therefore be summarised through several principles: respect for human autonomy; commitment to evidence and truth-seeking; responsibility for communication; recognition of legitimate pluralism; critical reflection before sharing information; and collective responsibility for the quality of the digital information environment.

The contemporary development of generative artificial intelligence and increasingly sophisticated forms of information manipulation makes these principles even more important. UNESCO, OECD and European institutions have all highlighted the growing significance of media literacy, digital competencies and resilience in responding to misinformation and emerging digital risks.[6][9][10]

Ultimately, a resilient young person is not one who rejects digital information, but one who can engage with it critically, ethically and independently. From this perspective, digital resilience is simultaneously a security capacity, an educational objective and a philosophical condition of personal autonomy. Strengthening it among young people can contribute to a more responsible digital culture in which technological development is accompanied by intellectual maturity, social responsibility and respect for human dignity.

References:

1. OECD. (2026). Growing up in the Social Media Age. OECD Digital Economy Papers, No. 385. Paris: OECD Publishing. https://doi.org/10.1787/a1132839-en. OECD.

2. Council of the European Union. (2026). Hybrid Threats. Brussels: Council of the European Union. Совет ЕС+1.

3. Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). The Landscape of Hybrid Threats: A Conceptual Model. Luxembourg: Publications Office of the European Union / European Commission Joint Research Centre. DOI: 10.2760/44985. hybridcoe.fi+1

4. Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe, DGI(2017)09. Совет Европы+1

5. Hybrid CoE. (2026). Hybrid Threats as a Concept. The European Centre of Excellence for Countering Hybrid Threats. hybridcoe.fi

6. Hill, J. (2022). Policy Responses to False and Misleading Digital Content: A Snapshot of Children's Media Literacy. OECD Education Working Papers, No. 275. Paris: OECD Publishing. DOI: 10.1787/1104143e-en. OECD

7. Pennycook, G., McPhetres, J., Zhang, Y., Lu, J. G., & Rand, D. G. (2020). Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. Psychological Science, 31(7), 770–780. DOI: 10.1177/0956797620939054. Sage Journals+1

8. Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. Humanities and Social Sciences Communications, 5, 65. DOI: 10.1057/s41599-019-0279-9. DOI+1

9. UNESCO. (2025). Media and Information Literacy and Digital Competencies. Paris: UNESCO. ЮНЕСКО+1

10. European Commission. (2026). Guidelines for Teachers and Educators on Tackling Disinformation and Promoting Digital Literacy through Education and Training. Brussels: European Commission. DOI: 10.2766/5220136. Европейская образовательная зона

11. UNESCO. (2025). Building Media and Information Literacy for a Resilient Uzbekistan. UNESCO Uzbekistan. ЮНЕСКО