Marcin M. Brocki
WSB University in Dąbrowa Górnicza
e-mail: mbrocki94@gmail.com
ORCID: 0009-0002-0576-5224

DOI: 10.26410/SF_2/25/9

DIGITAL RISKS FOR CHILDREN AND ADOLESCENTS IN POLAND IN 2024 IN LIGHT OF THE 4 CS FRAMEWORK: AN ANALYSIS OF NATIONAL REPORTS

Abstract

The article analyses nationwide research from 2024 on the risks to which children and young people are exposed in the digital environment, using the 4C model. The study is based on reports entitled *Teenagers*, *Internet children*, and data from Dyżurnet.pl and the Office of the Ombudsman for Children's Rights. The results indicate that the 4C model can be used to classify threats and their nature, but it is difficult to create a matrix combining both approaches. The most common threats are harmful content, cyberbullying, and sexual threats, while there is a lack of data on commercial and contractual threats. The author emphasizes the need for in-depth research on child profiling, aggressive marketing, gambling mechanisms, as well as radicalization and more in-depth analysis of the risks associated with artificial intelligence.

Key words

digital safety, children and youth, 4C model, cyberbullying, harmful content

Introduction

The dynamically changing online environment creates a space for users in which development potential coexists with various forms of threats. Children and young people are a particularly vulnerable group, as their intense emotional and social development overlaps with their growing exposure to digital technologies. Although knowledge about the associated risks in Poland is steadily expanding, it remains scattered across many publications and reports, which creates a need to organize it.

The scale of the problem is illustrated by the results of nationwide surveys. The report *Internet dzieci* (Children and the Internet) notes that 85.6% of children aged 7–14 use the Internet, and in the 15–18 age group, this percentage is close to 100%[1]. In turn, the report *Nastolatki* (Teenagers) published by the Digital Citizenship Institute Foundation indicates that students in grades 7–8 of primary school and grades 1–2 of secondary school spend an average of 4 hours and 59 minutes in front of a screen on weekdays and 5 hours and 16 minutes on weekends. Most of them received their first smartphone at the age of 9–10, and about 40% before the age of 9[2].

It is worth noting that, unlike adults, adolescence is characterized by "multifaceted and intense changes" and tasks that "have a social dimension and are associated with gaining emotional independence"[3]. Early and frequent contact with the internet makes young users particularly vulnerable to threats that can disrupt this process, endanger their health and, in extreme cases, their lives. Such threats include misinformation, radicalization, cyberbullying, and exposure to age-inappropriate content.

These phenomena are also widely discussed in international literature. Research conducted by EU Kids Online, the International Telecommunication Union, and the Organization for Economic Co-operation and Development, among others, indicates that the internet is now one of the key environments in which young people operate. This requires systematic analysis of both the opportunities and threats associated with this ecosystem. Attention is drawn to the growing complexity of the digital environment, where risks arise not only from interpersonal relationships, but also from platform architecture, business models, and data processing methods.

Polish studies on the digital safety of children and young people emphasize that cyberspace is now an important area for socialization and relationship building. This is pointed out, among others, by B. Marciniec and D. Marczuk[4], who

1 M. Bigaj, K. Ciesiołkiewicz, K. Mikulski, A. Miotk, J. Przewłocka, M. Rosa, A. Załęska, *Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie*, Warsaw 2025, p. 30.

2 A. Ładna, K. Kamiński, K. Rosłaniec, A. Wrońska, M. Błażej, A. Jankiewicz, F. Konopczyński, M. Nawrot, *Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców*, NASK – National Research Institute, Warsaw 2025, pp. 27–28.

3 A. I. Brzezińska, K. Appelt, B. Ziółkowska, *Psychologia rozwoju człowieka*, Sopot 2016, pp. 245–247.

4 B. Marciniec, D. Marczuk, "Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej", *Rozprawy społeczne* 2015, Vol. IX, No. 2, pp. 34–38.

highlight the growing importance of the online environment in the everyday lives of young people. A similar view is presented by J. Pyżalski[5], who shows that the online activity of adolescents (teenagers) combines both developmental and civic potential and various forms of risk.

Despite the growing number of national publications, their content often remains scattered and covers only selected aspects of risk. Some studies focus on legal issues[6], while others focus on the socialization and cultural dimensions[7]. However, there is still a lack of analyses that systematize threats in accordance with recognized international frameworks. Of particular importance here is the 4C classification (Content, Contact, Conduct, Contract) proposed by S. Livingstone and M. Stoilova[8], which provides a structured and comparable approach to the risks associated with children's use of the internet. This classification includes the following categories:

- Content – harmful material, e.g., pornography, harmful content, misinformation.
- Contact – the risk of contact with strangers online, e.g., grooming, phishing of minors, recruitment into criminal groups.
- Conduct – risks resulting from the actions of users themselves, e.g., cyberbullying, sharenting, doxing.
- Contract – threats resulting from the commercial exploitation of children, e.g., microtransactions, online gambling, advertising profiling of minors.

The authors also propose an additional dimension of classification, referring to the nature of the risk – aggressive, sexual, axiological, and commercial. However, the use of this perspective requires a detailed description and classification of threats, which is difficult due to the limited availability of data. In this context, there is a research gap regarding the lack of a synthetic analysis of Polish data in relation to the 4C model. Filling this gap would allow for a more precise assessment of the scale of individual types of risks and reliable comparisons with the results of international studies, in which this model is increasingly used.

The aim of this article is to organize knowledge about threats to children and young people on the Internet in 2024 by analyzing nationwide reports in relation to the 4C model. The article also aims to identify types of threats and areas requiring further research based on the results of the aforementioned summary in order to better understand the situation of young people in the digital world.

5 J. Pyżalski, "Positive Internet Use and Online Civic Engagement versus Active Involvement in Selected Online Risks – how are both connected in adolescents from six European countries?", *Psychology, Society & Education* 2023, Vol. XV, No. 3, pp. 16–17.

6 See: M. Olchanowski, "Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni…", *Zbliżenia Cywilizacyjne* 2017, Vol. XIII, No. 3, pp. 56–68.

7 See: M. Konopczyński, F. Konopczyński, "Młodzież, internet, socjalizacja…", in: A. Wrońska, R. Lew-Starowicz, A. Rywczyńska (eds.), *Edukacja – relacja – zabawa*, Warsaw 2019, pp. 21–25.

8 S. Livingstone, M. Stoilova, *The 4Cs: Classifying Online Risk to Children*, Hamburg 2021, p. 12.

Methodology

The study was based on a review of literature and reports addressing the threats faced by young people in Poland. The search included publications meeting the following criteria:

- The research was conducted in 2024 and was nationwide in scope.
- It concerned the issue of children and young people's exposure to risks associated with internet use.

On this basis, the following reports were selected for further analysis:

- Teenagers. Report from a nationwide survey of students and parents, published by NASK in 2025.
- Children's Internet. Report on monitoring the presence of children and young people on the Internet, published by the Digital Citizenship Institute Foundation in 2025.

The next step was to identify the behaviors and phenomena described in the reports that indicate the exposure of the surveyed children and young people to the risks of using the Internet, taking into account the scale of occurrence of these phenomena. The identified elements were then organized according to the 4C model concept.

The threats organized in this way made it possible to identify the categories of risks with which young people have the most frequent contact, as well as those that require greater attention due to the limited availability of empirical data.

The study was based largely on the use of theoretical methods, in particular: analysis – used to break down the issue into its constituent elements, including the identification and organization of threats found in the reports; synthesis – enabling the combination of the identified information and the assignment of the identified threats to the appropriate categories of the 4C model; abstraction – used to extract key elements from extensive research material; and generalization and inference, which allowed for the identification of the most important threats currently faced by children and young people, as well as the identification of areas requiring further empirical research due to the limited scope of available data[9].

Threats to children and young people online in Poland and the 4Cs concept

The Teenagers Report. a report from a nationwide survey of students and parents, published by NASK, focuses on how young people (students in grades 7–8 of primary school and grades 1–2 of secondary school) perceive and experience the digital world, especially the internet, and how parents assess their children's participation in the virtual space. Analysis of this document allows us to extract data relevant for further research:

9 See: J. Apanowicz, *Metodologia ogólna*, Gdynia 2002, pp. 23–28.

- 28% of teenagers declared that they had been victims of cybercrime, including:
  - account hacking – 12%,
  - theft of virtual goods – 8%,
  - hacking/data theft – 7%,
  - threats of violence in the real world – 6%,
  - blackmail/attempted extortion – 5%,
  - online shopping fraud – 5%,
  - impersonation/identity theft – 4%,
  - cryptocurrency fraud – 2%.
- Approximately 38–42% of respondents have experienced various forms of cyberbullying, including:
  - name-calling – 29%,
  - ridicule – 19%,
  - humiliation – 18%,
  - threatening – 13%,
  - blackmail – 13%,
  - disseminating compromising materials – 9%,
  - impersonating the subject – 8%.
- 22% of students declared that they had seen pathostreams at least once.
- 26% had participated in online challenges.
- 41% had encountered pornography; the average age of first contact was 11 years and 3 months.
- Sexting: 28% of students received nude or semi-nude photos from someone, and 5% sent such material themselves.
- Grooming: 11% of respondents had contact with adults they met online, of which 28% did not inform anyone about it.
- 67% of respondents declared that they had seen deepfake material at least once, i.e., material generated by artificial intelligence to mislead the recipient[10].

The report *Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie* (Children on the Internet. Report on monitoring the presence of children and young people on the Internet), prepared by the Digital Citizenship Institute Foundation, presents the results of cross-media research recording actual Internet use on devices. Two age groups were distinguished: children (7–14 years old) and adolescents (15–18 years old). From the perspective of this article, the key data from the report include:

- 53.8% of adolescents (aged 15–18) and 51.3% of children (aged 7–14) have been exposed to pornography, with 25% of this group viewing such content at least once a month,

10 A. Ładna et al., *Nastolatki…*, op. cit., pp. 67, 69, 81, 85, 88, 92, 95, 101, 103, 137.

– 1.6 million children aged 7–12 use social media before reaching the age of 13, which represents over 66% of this population. It is worth noting that most social networking sites specify a minimum user age of 13 in their terms and conditions[11].

In the context of the nationwide survey conducted in 2024, it is worth mentioning two additional sources that broaden the perspective, although their full use in this analysis was difficult.

The first is the study Let's look at the internet through the eyes of children, commissioned by the Ombudsman. Respondents (aged 12-17) indicated that the most harmful threats in their opinion were: hate speech (84%), stalking (77%), and publishing someone's image without their consent (74%). These concerns partly overlap with the threats identified in the reports Teenagers and the Internet and Children and the Internet, concerning cyberbullying and sexting[12].

Another valuable source is the report on the activities of the Dyżurnet.pl team for 2024. It records the following incidents related to the sexual exploitation of minors:

– content depicting the sexual abuse of children – 11,147 incidents,
– content presenting children in a sexual context (e.g., modeling, posing) – 1,012 incidents,
– promotion of pedophilic activity – 29 incidents,
– child grooming – 26 incidents[13].

These data highlight the importance of research on sexual threats, especially in the context of pedophilia, grooming, and child pornography.

Table 1. Threats to children and young people from the perspective of the 4C concept

4C	Threat	Exposure of respondents to the threat expressed as a percentage.	Source
Content	Exposure to pornography	41% (primary school grades 7-8, secondary school grades 1-2), 53.8% (ages 15-18), 51.3% (ages 7-14)	Teenagers, Children's Internet
	Pathostreams	22%	Teenagers
	Participation in challenges	26%	Teenagers
	Social media <13 years old	over 66% (7-12 years old)	Children's internet use
	Deepfake	67%	Teenagers

11 M. Bigaj et al., *Internet dzieci…*, op. cit., pp. 41, 52–53.

12 Biuro Rzecznika Praw Dziecka, *Spójrzmy na internet oczami dzieci. Wyniki badań RPD*, Warsaw 2025.

13 Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, *Raport 2024. Dyżurnet.pl*, Warsaw 2025, p. 18.

4C	Threat	Exposure of respondents to the threat expressed as a percentage.	Source
Contact	Grooming – contact with adults	11%	Teenagers
	Sexting – receiving sexual content	28%	Teenagers
	Threats of violence in real life	6%	Teenagers
Conduct	Name-calling	29%	Teenagers
	Ridicule	19%	Teenagers
	Humiliation	18%	Teenagers
	Threatening	13%	Teenagers
	Blackmailing	13%	Teenagers
	Compromising materials	9%	Teenagers
	Impersonation	8%	Teenagers
	Sexting – sending photos	5%	Teenagers
Contract	Account hacking	12%	Teenagers
	Theft of virtual goods	8%	Teenagers
	Hacking / data theft	7%	Teenagers
	Shopping fraud	5%	Teenagers
	Money extortion	5%	Teenagers
	Identity theft	4%	Teenagers
	Cryptocurrency fraud	2%	Teenagers

Source: own study.

A comparison of the reports on teenagers and the internet allows us to conclude that the Content category is the one with which children and young people in Poland have the most frequent contact (see Table 1). The most frequently mentioned threats are deepfakes, exposure to pornography, pathostreaming, and participation in online challenges. It is worth noting that not every challenge is negative (e.g., the second edition of the #Hot16Challenge in Poland), but the reports treat this phenomenon in a general way, which is due to the specific nature of the research.

An important category, although dominated by one phenomenon, is Conduct, in which cyberbullying remains the most common problem – almost every second student surveyed was a victim of it.

The Contact category, on the other hand, covers threats arising mainly from sexual relationships and contact with unknown adults.

The last category, Contract, was dominated by cybercrime phenomena, especially account and identity theft.

It is noteworthy that categories such as Contact, Contract, and Conduct turned out to be quite monothematic. This may indicate the need to consider a broader or more accurate spectrum of threats in future studies conducted by both the institutions indicated and independent researchers. This would provide a more complete picture of the threats faced by young Internet users.

The monothematic nature may also result from the general nature of the threats declared by participants, which makes it difficult to classify them according to the 4C model. The reports are dominated by references to cyberbullying, sexual threats, and cybercrime, while others, such as participation in challenges or deepfakes, remain too broadly described. Deepfakes appear in the report as a threat, but their nature has not been clearly defined, which further complicates their classification in the 4C model. This is also worth noting when analyzing deepfakes in the Teenagers report. Deepfake content encountered by respondents was most often used for jokes, ridicule, deception, and misinformation[14]. It is worth noting that this is the opinion of students on the use of this phenomenon, and not their actual exposure to this threat in this capacity. The current design of the study allows for a relatively precise identification of sexual and commercial threats, while it is more difficult to clearly classify those related to values and aggression so that they do not overlap between the 4C categories.

International reports mention other types of threats which, in the author's opinion, should be included in future Polish nationwide studies, e.g.:

Content:
- materials related to self-harm and suicide[15],
- violent content[16],
- extremist content[17],
- disinformation[18].

Contact:
- recruitment for criminal activities[19].

Conduct:
- doxxing[20].

14 A. Ładna et al., *Nastolatki…*, op. cit., p. 140.

15 D. Smahel, H. Machackova, G. Mascheroni et al., *EU Kids Online 2020: Survey Results from 19 Countries*, London 2020, pp. 61–62.

16 Office of Communications, *Children's Media Literacy Report 2024*, London 2024, pp. 23–24.

17 Ibid, p. 3.

18 Ibid, pp. 34–35.

19 European Union Agency for Law Enforcement Cooperation, *The Recruitment of Young Perpetrators for Criminal Networks*, The Hague 2024, pp. 2–3.

20 D. Smahel et al., *EU Kids Online 2020…*, op. cit., pp. 70–72.

Contract:
- loot boxes and other gambling-like mechanics[21],
- aggressive, hidden marketing aimed at children[22],
- profiling of children[23].

These are examples of threats that have been identified both in Poland and internationally. Many of them are changing rapidly and overlap between categories, which indicates the need for systematic monitoring. This list is not exhaustive – it is a proposal for further research.

Summary

The aim of this article was to organize knowledge about the threats described in nationwide reports on children and young people on the Internet in 2024 by analyzing them in relation to the 4C model and, based on the data obtained, to indicate possible directions for further research. Extending the analysis to include earlier studies and regional reports could enable a more comprehensive understanding of the phenomenon, observation of trends, and, in the longer term, the proposal of an original classification of threats based on the 4C model adapted to the Polish reality.

The risks described in the reports can be assigned to the 4C model based on the risk categories "Content, Contact, Conduct, and Contract." This allows us to conclude that the risks faced by young people are diverse. a nationwide study conducted in 2024 analyzed the exposure of children and young people to a number of risky phenomena encountered by a large proportion of young respondents. However, it is worth noting a certain concentration around the risks studied – issues related to cyberbullying, harmful content, and sexual threats dominated among them.

The greatest data deficiency is visible in the Contract category, where reports focused mainly on cybercrime issues. Future studies should also analyze phenomena such as the use of so-called loot boxes or other gambling-like mechanisms, as well as the problem of profiling children on the internet and their exposure to aggressive marketing. The rapidly developing threats associated with artificial intelligence should also be taken into account. The reports address both this issue and the way in which children and young people use these technologies. In the context of threats, it was mainly considered as deepfake, which is a very accurate perception of the problem. At the same time, it is worth considering the nature of such content in the context of deepfakes, e.g., radicalizing, pornographic, disinformation, inciting violence. With the development of this technology, it is also worth monitoring new threats that may emerge in connection with the development of language models and other AI-based tools.

21 Organisation for Economic Co-operation and Development, *Consumer Vulnerability in the Digital Age*, Paris 2023, pp. 20–21.

22 Ibid, pp. 36–38.

23 Ibid, pp. 24–26.

It is worth noting that the classification of threats according to their nature (e.g., aggressive, sexual, axiological, commercial) is currently difficult due to the limited level of detail of the available data. With the current state of knowledge, it is possible to classify threats according to the 4C model types, but creating a complete, non-duplicative matrix of threat categories and nature would require more precise data. Obtaining such data may be challenging, among other things due to the fact that the respondents in these studies are minors.

Nevertheless, in the author's opinion, such an effort is necessary. It would allow for a more detailed understanding of the nature of the risks faced by children and young people in the digital environment and for the development of a coherent research framework adapted to the specificities of the Polish social context.

Bibliography

Apanowicz J., Metodologia ogólna, Gdynia 2002.

Bigaj M., Ciesiołkiewicz K., Mikulski K., Miotk A., Przewłocka J., Rosa M., Załęska A., Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie, Warszawa 2025.

Biuro Rzecznika Praw Dziecka, Spójrzmy na internet oczami dzieci. Wyniki badań RPD, Warszawa 2025.

Brzezińska A. I., Appelt K., Ziółkowska B., Psychologia rozwoju człowieka, Sopot 2016.

European Union Agency for Law Enforcement Cooperation, The Recruitment of Young Perpetrators for Criminal Networks, The Hague 2024.

Smahel D., Machackova H., Mascheroni G., Dedkova L., Staksrud E., Ólafsson K., Livingstone S., Hasebrink U., EU Kids Online 2020: Survey Results from 19 Countries, London 2020.

Konopczyński M., Konopczyński F., „Młodzież, internet, socjalizacja – w perspektywie współczesnych paradygmatów społecznych", w: A. Wrońska, R. Lew-Starowicz, A. Rywczyńska (red.), Edukacja – relacja – zabawa. Wieloaspektowość internetu w wymiarze bezpieczeństwa dzieci i młodzieży, s. 14–39, Warszawa 2019.

Livingstone S., Stoilova M., The 4Cs: Classifying Online Risk to Children, Hamburg 2021.

Ładna A., Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców, NASK – Państwowy Instytut Badawczy, Warszawa 2025.

Marciniec B., Marczuk D., „Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej", Rozprawy społeczne, t. IX, nr 2, 2015, s. 34–38.

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Raport 2024. Dyżurnet.pl, Warszawa 2025.

Office of Communications, Children's Media Literacy Report 2024, London 2024.

Organisation for Economic Co-operation and Development, Consumer Vulnerability in the Digital Age, Paris 2023.

Olchanowski M., „Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni na podstawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej na lata 2017–2022", Zbliżenia Cywilizacyjne, t. XIII, nr 3, 2017, s. 56–69.

Pyżalski J., „Positive Internet Use and Online Civic Engagement versus Active Involvement in Selected Online Risks – how are both connected in adolescents from six European countries?", Psychology, Society & Education, t. XV, nr 3, 2023, s. 10–18.

Telemedia Management GmbH, Safeguarding Children Online: a Service-Specific View on Risks and Parental Attitudes, Geneva 2023.

About the Author

Marcin Brocki is a doctoral researcher in security studies at the WSB Academy, whose research interests national and human security, safety education, and youth cybersecurity. His academic background is complemented by practical experience within crisis-management structures, including work at the Emergency Notification Center, as well as by teaching activity in the fields of security and civic education.