DOI: 10.35765/mjse.2023.1223.18
Submitted: 04.05.2022
Accepted: 11.04.2023
Published: 30.06.2023

Marek Górka
https://orcid.org/0000-0002-6964-1581
Koszalin University of Technology, Poland
marek_gorka@wp.pl

Multidisciplinary Journal of School Education • Vol. 12, 2023/1 No. 23
Skills, Competences, Values in Education: New Perspectives

Design of an Innovative Model of Cooperation Between Schools and the Public for the Cybersecurity of Children and Adolescents

(pp. 413–432)

Abstract

The article deals with the prevention of cyber threats to children and adolescents through the cooperation of public institutions, which can be one of the key factors in increasing safety in the virtual world. The purpose of the article is to evaluate the effectiveness of the model of cooperation of local government institutions. The novelty of the research problem lies in the attempt to practically apply the exchange of knowledge and experience between local institutions, with a particular focus on cybersecurity education. The analysis is based on students' responses from surveys conducted between 2019 and 2021, making it possible to apply quantitative analysis and to characterize the changes in the incidence of cyberthreats. The second research tool is qualitative analysis, through which we can learn about the impact of educational activities on the level of awareness of cybersecurity. The research period has three stages: the first is before the introduction of remote learning, the second is during the pandemic and remote learning, and the third is the return to in-school learning. The research analysis deals with the problem of digital threats that the modern school, with the support of other public institutions, has to face.

Keywords: education for cybersecurity, cybersecurity, innovation, collaboration, public sector

ISSN 2543-7585 e-ISSN 2543-8409

This article presents an analysis of the cooperation at the local government level between the police headquarters in Szczecin, Gdansk and Koszalin and the Koszalin University of Technology and selected schools from northern Poland, in the area of combating cyber threats among children and adolescents for the period 2019–2021. The second important goal of the research is to investigate whether this prevention, applied as a result of cooperation between public institutions, contributed to increased safety in the virtual world. The results indicate a significant relationship between educational activities in the field of cybersecurity and the occurrence of threats among young Internet users. The article addresses the problem of implementing cybersecurity education, particularly in towns and cities with populations of up to 100,000. The project is a model of cooperation among local government institutions, which can also be replicated in other areas of local development. In other words, it is a form of seeking opportunities to develop cooperation which can be applied in other areas related not only to security, but also to local development.

The perceived need – and the social pressure – resulting from cyber threats publicized by local media was one of the factors that led to the cooperation between local institutions interested in security. This project can also serve as an example for other institutions from other regions of the country which operate in the field of digital education. It also shows how institutions working together can jointly work on contemporary cybersecurity challenges. The article describes a model for developing public sector innovation from the perspective of cybersecurity education. The practical application of the project shows the advantages that result from cooperation among public sector institutions. It is also worth noting that this issue touches on the problem of ongoing changes in public administration. The aim is therefore to analyze innovation, which is also in this case a form of public partnership.

As an aside, it is worth pointing out how this paper defines the term cybersecurity, which is constantly evolving and is often a contentious issue among researchers. Given the far-reaching implications of the development of cyberspace for society, the term used in this paper encompasses

ISSN 2543-7585 e- ISSN 2543-8409

preventive measures against cyber threats faced by young people, especially related to cyberbullying.

Cooperation between institutions

Media stories that warn about attempted fraud in cyberspace prove how important cybersecurity is in everyday life (Domurat, 2012). The advent of online communication, and with it much broader access to smartphones and computers, has changed the previous culture and values and has allowed for new ways to commit crime. A lack of awareness about the dangers of the Internet can contribute to many problems, such as losing confidential information, identity theft, and cyberbullying. The literature in the area of cybersecurity is diverse and informative. Many papers discuss a range of issues connected with cyberbullying in various forms. They also indicate that understanding cybersecurity depends heavily on an interdisciplinary approach to researching the topic. A prerequisite is therefore to use both technical and social sciences (Holt, 2016; Gillespie, 2016; Holt et al., 2015; Wall & Williams, 2014).

Awareness of cyber threats is a variable phenomenon that depends on many sociodemographic factors, such as age, gender, education, and place of residence. Prevention is also an important element, based primarily on education. This problem becomes even more important in the context of the modern IT revolution, resulting in widespread and easy access to technology. The mass media often report on problems or tragedies among young people that result from a lack of awareness of the dangers lurking in the virtual world. The attitude of teachers and educators is quite enigmatic and unclear, manifested as grief and shock in a sudden situation caused by the drama (Torgal et al., 2021; Kearney et al., 2022). This is in many cases a reaction that is too late and rather focused on minimizing the problems that have already occurred. There is a noticeable lack of cybersecurity education of a preventive nature. Taking into account the above factors, it is worth considering how effective the cooperation of police, academia and schools can be at preventing online fraud.

The police force is an institution that has a duty to ensure the safety of its citizens. Cyber threats are usually dealt with in the Polish police by the Department of Economic Crime, which in cyberspace works toward protecting copyrights and preventing and combating fraud, the most common victims of which are young people. However, with all the involvement of the police, there is a lack of financial resources, technological resources, and specialists in not only information technology, but also Internet psychology. In addition, in the last two years there have been many people searching social networks, chat rooms and forums on their own initiative in order to root out fraudsters. On the one hand, this has a prophylactic and somewhat preventive effect, discouraging individuals from the inclination to commit fraud or deceive others. Nevertheless, such provocations, as well encouraging certain online behaviors, can be seen as breaking the law – even if done with good intentions. Thus, the key issue addressed in this article is changing the existing actions in the field of cyber threats, which so far have not had the expected effect – as seen by the research results. The second important issue is to show how researchers can get involved in cybersecurity education.

The involvement of academia can improve the chances of success for an innovative model in the public sector. In this case, the goal and the challenge becomes discovering processes and phenomena that actually occur in society. The project also has a scientific dimension, because it shows which activities work and which do not. This is important because public sector innovation can be interpreted as gaining knowledge in an unverified area.

Innovation as a source of success

Since the systemic transformation that began in 1989, public administration has gone through successive stages of change, as in many Central and Eastern European countries. The main idea guiding these evolutionary processes was to move away from the bureaucratic model of administration towards managing public institutions as enterprises.

The administrative reform of 1999 and Poland's accession to the European Union in 2004 accelerated the changes by decentralizing and liberalizing local policy. Moreover, the need to obtain EU funds, the purpose of which was and still is to finance local government investments, had a great impact. This led to a kind of competition for financial support of selected investments, as a result of which projects became more and more competitive. Therefore, innovativeness refers not only to new products, but also to services, processes, business models, markets, or sources of supply that provide a specific institution with a competitive advantage over other organizations.

In a complex and dynamic reality influenced by globalization and technology, the management and development of public institutions increasingly require rethinking and innovation. The contemporary emphasis on innovation in the public sector is gaining importance, as indicated by many authors (Sanina et al., 2021; Trček & Likar, 2014). Innovation is understood as being inseparable from the concept of change, novelty, reform, or an idea perceived as "new."

Innovations are considered to be the most diverse facts, processes, and phenomena of a technical, organizational, social, or psychological nature. This diverse and general understanding of innovation results both from the short tradition of research on innovation and the diversity of theoretical approaches (Stawasz & Niedbalska, 2011). Innovation brings with it additional requirements to be met, such as customer satisfaction, market needs and efficiency in delivering public services (Webster, 2004). Innovation refers to something new, dynamic, and not yet fully known. The existing reality is thus transformed as a result of a new idea. Implementing a project in public space, whose key factor is cooperation between institutions with different tasks and functions, requires a change in the way administration is managed. It consists primarily in a transition from a model based on issuing orders and commands and rigid adherence to designated responsibilities to a managerial model based on a creative, open approach to challenges. This new managerial model is becoming increasingly important in the planning and implementation of social projects (Toivonen & Tuominen, 2009).

ISSN 2543-7585 e-ISSN 2543-8409

The conditions conducive to innovation in the public sector are highly dependent on the level of economic development, the maturity of civil society, financial capacity, and the management in the local government institution (Webster, 2004). There are also social/cultural challenges in reforming an administrative system. There are difficulties to overcome, especially in an environment where there is a strong bureaucratic foundation (Unceta et al., 2020; Pillay, 2008; Schick, 1998). Project implementation therefore forces many public institutions to go beyond the statutory framework. Creating new opportunities also contributes to new ways of creating norms and values in the institution.

Innovation is a form of competition in the modern economy, but the public sector (unlike in politics) does not have to compete to "attract customers" (Plamer, 1993; Smith, 2016). This is primarily because administrative institutions have a monopoly on the services they provide. Innovation implies uncertainty, which is the result of certain assumptions, which in theory assume certain outcomes and only through practical testing verify the previous assumptions.

Despite the fact that many offices have as part of their duties or mission the establishment and maintenance of cooperation, in practice they are implemented differently. Many organizations do not have appropriate conditions to effectively implement the cooperation model. That is why – one can assume – it is emphasized in the literature that the public sector suffers from an innovation deficit (Lember et al., 2015; Potts & Kastelle, 2010). While in private organizations the impulse for change is improving production or economic gain, usually in the public sector activities that work well do not change or evolve much more slowly.

Factors leading to project failure

Following best practices is no guarantee that an idea will be implemented very well – even in the private sector. Barriers caused by bureaucracy can lead to the functioning of even the best projects being quickly paralyzed at the very beginning. The implementation of certain innovations depends on selected units belonging to public institutions. However, it is worth asking whether a change in the approach to task implementation would interfere with the previous public management, based on stereotypes, habits, and thought patterns. Despite some changes, there are still psychological and cultural barriers resulting from a centralized, hierarchical model of authority. Surveys, observations, and overt and covert interviews were conducted with officials of the West Pomeranian Province between January 2019 and June 2020. The research shows that the principles of reform can be accepted and applied as long as they do not contradict other "established" and traditional work principles. The tendency to think that innovation is connected with unavoidable problems was observed in at least 3/4 of the surveyed local administration employees. The conviction that any change entails costs, not only financial, but also in the form of time or work effort, is the prevailing attitude among many officials, which negatively influences the perception of any changes. This view is also confirmed by the analysis of researchers who put forward similar theses that any change raises concerns among public sector employees resulting from the evolutionary process (Cole, 1988; Sanina et al., 2017).

In addition to the psychological and cultural barriers, it is necessary to take into account the statutory provisions that determine the nature of administrative employees' work. Bureaucratized organizations tend to be inefficient and inflexible at meeting collective needs. Often the public perception of public administration is also negative because of its failure to meet the needs arising from modern society, among other things.

Risks arising from introducing changes are encountered because of frameworks strictly defined in laws, the status of institutions, customs and social norms, and top-down orders. This constructed reality rewards mediocre or simply passive attitudes. Avoiding instability or work paralysis caused by the introduction of changes are common practice (Sanina et al., 2017). In summary, the possibility of success of a particular innovation is less appreciated than the guarantee of avoiding problems and unpleasant events resulting from the changes it entails (Potts & Kastelle, 2010; Lember et al., 2015).

ISSN 2543-7585 e- ISSN 2543-8409

ISSN 2543-7585 e- ISSN 2543-8409

Of course, there are certain levels in institutions providing public services that require developed and proven templates to guarantee the performance of the task, such as in the case of administrative matters related to civil registration, tax settlements, social security, or health services. There are also implications arising from the fact that an administrative institution is part of a larger whole in the public sector and is obliged to fulfill its clearly defined legal obligations. In other words, innovation is not central to the public sector, for failure to innovate rarely has disastrous consequences. Nor is the public sector entirely guided by the principles of economic efficiency, which in this case are understood as minimizing losses and maximizing profits. In the private sector, success is interpreted primarily as profit maximization, but innovations in the public sector are not perceived in this way. Thus, the conclusion is that new ideas should be experimented with in a controlled manner in order to minimize unintended harm and to maximize expected value.

The public sector is a set of institutions funded by the state, i.e., by public funds. In this situation, certain failures can be problematic, and in addition to the financial costs, they may be met with a lack of understanding from the media or the political opposition. Most institutions implement changes resulting from changes in legislation. In this way, the responsibility for possible failures is minimized. That is why local self-governments most often choose actions which do not carry a high risk of failure or loss of financial resources, but which guarantee the possibility to promote themselves. The priority is therefore stable functioning of the institution without any problems or unforeseen events.

By its very nature, public administration does not have competition from other institutions that would compete for market share in services, such as the County Office, Municipality or City Hall, Tax Office, Social Insurance Institution, Police, Army, etc. The exception here is education, in which private schools compete with public institutions for students. The growing competition for students between higher education institutions (including public ones) should also be noted. Each institution tries to offer the most attractive education. Thus, an increasing degree of innovation can be observed in the education system.

"Education For Cybersecurity" project

The cybersecurity project was originally planned for the period 2019–2021, but there is a need for long-term prevention, as indicated by factors such as the continuously emerging threats, the rising number of young Internet users, and the need for continuing education in this area. In accordance with this approach, the intention of the project was to involve as many partners as possible in initiating an integrated process of knowledge and experience sharing and to further explore the potential of cooperation between public institutions. The aim of the project is to demonstrate a new model of cooperation between institutions that will demonstrate its usefulness and relevance to the problems in question. The project also gives the opportunity to view cyber threats in a new way.

Innovation in this case is understood as a special kind of collaboration between institutions. This raises the question of how institutions can engage and participate in the development of cybersecurity education. In the case of this project, the uniqueness of the model lies in the exchange of knowledge and experience and in the sharing of skills (Kravariti & Johnston, 2020; Horbacha et al., 2013). The implementation and outcomes of such collaborations are particularly beneficial to the local community. More importantly, the project also provides an opportunity to verify the level of service, that is, how effectively public institutions are functioning. By noting joint activities, such as training courses, conferences, and meetings with youths, as well as by conducting community interviews, the information thus obtained can be used to measure the effectiveness and efficiency of the actions taken.

A significant share of social, cultural, and security-related problems are very complex in nature and attempts to analyze them in only one context cannot explain the complexity of the whole situation. Therefore, there is a need to analyze events from different angles. Such a perspective can be provided by employees working in different types of institutions whose tasks complement each other. Such a project offers many advantages for each of the participating institutions.

The employees of educational and research institutions feel that society's expectations of their profession are constantly growing and changing very quickly, while they are simultaneously obliged to remain an expert in their given field. Interviews with educators working in schools reveal that there is a great need to implement and carry out lessons in the field of online safety. Therefore, this project is a kind of response to the above-mentioned social expectations. It means mutual support of institutions with knowledge and experience, thanks to which it is more efficient to achieve the cybersecurity goals.

The project provides an opportunity to conduct a case study using a questionnaire interview; it will indicate which methods of social communication and forms of cybersecurity prevention are effective and should be continued. There is also the possibility to include NGOs in the project. Convinced of the value of the undertaking of researchers, local authorities, and uniformed services, NGOs may constitute another important element in developing cooperation in cybersecurity education.

It is crucial that the project emphasizes institutional cooperation when creating new practices to counter online threats. In other words, for the success and continuation of the project, a real commitment from all the actors involved is essential. To this end, a specific form of agreement is needed that identifies the institutions involved and defines their roles, tasks, the scope of their involvement, and the use of their resources. Of course, it is also important to identify a project facilitator, whose responsibility is to ensure an effective and understandable flow of information between the parties involved and to oversee the next steps in the implementation process. The research also reveals a gradual professionalization of relations between the cooperating institutions. Therefore, another important task of the project is to promote institutionalized cooperation between the public entities responsible for cybersecurity education. The second, obvious group of recipients are young people, to whom the effects of this cooperation are and will be directed.

Convincing employees, especially those in managerial positions, to use new, unproven methods remains a major challenge. The introduction of changes depends to a large extent on the way the institution is managed, which may take a hierarchical and bureaucratic form of giving orders or may follow a managerial, open and, motivating model in the relations between superiors and employees. Innovation is a kind of call for those in leadership positions in the public sector to expand the scope of the institutions they lead (Cooke, 2017). An important issue remains effectiveness: without the real involvement of the employees in the participating institutions and solely following a top-down order structure the quality of the program can be significantly impacted.

Methodology and structure of the project

The first part of the project consists of two elements, the questionnaire and the scientific conferences. An anonymous online interview with schoolchildren was conducted in March/April 2019 to identify the knowledge and awareness among young people. Two weeks later, a scientific conference and a series of meetings with youths were organized. The next survey was conducted in April, before the planned scientific conference, and a series of lessons in schools again took place in May 2020. The third survey, in March 2021, was conducted prior to another academic conference and a series of meetings with students in schools.

The academic conferences addressed public safety issues, including cyber threats. They were an opportunity for representatives of the scientific community, uniformed services, and school educators to speak. Junior high school students also participated in the project. The conferences and lessons were aimed at raising awareness and enriching knowledge about cybersecurity through information and experience from uniformed services officers, civil employees, and researchers working in the field of public security issues.

In summary, the innovation of the project and the enormous benefit of sharing knowledge, needs, expectations, and information occurred between three community groups: (1) uniformed services, (2) academia, and (3) educators and middle school students. Residents of Szczecin, Gdańsk, and Koszalin also took the floor during panel discussions at the academic conferences. The very knowledge of the needs and expectations of the residents (e.g., NGO activists or members of neighborhood clubs) was a valuable, unique source of information for the uniformed services, allowing them to identify actual or possible local threats and to concretize and define the goals of the services in the local community. On the other hand, the knowledge and experience of public officers (scientists, police, municipal guards, border guards, etc.) helped the conference participants to become aware of and familiar with cybersecurity issues.

During the conferences, employees of schools and representatives of other pedagogical institutions were present, as were young people themselves, whose knowledge was a source of information for the topics raised in the discussion panels. The conferences initiated the creation of a unique public forum, which provided a platform for the exchange of comments, knowledge, and experiences on improving and correcting activities in local security for the future.

The second part of the project involved face-to-face discussions and meetings with young people at schools. Each such event lasted two hours. During the first hour, the legal consequences of irresponsible behavior on the Internet were discussed, as well as whom victims of cyberbullying can directly turn to. The second hour was conducted by a representative of the Koszalin University of Technology, who talked about how to behave when receiving suspicious messages and invitations from strangers. An important component of the lectures was to draw attention to behavior that should be avoided during online contact with other users.

The first part of the project consisted of a community interview (through online tools) and a scientific conference. The information gathered in this way – based on a survey, interview, and online conversations with young people and educators – led to a common educational strategy, which was useful in the next stage of the project. The second step was online lessons in schools, which were in the form of lectures, exercises, and discussions. The results indicate a gradual process of increasing awareness of the dangers lurking in the virtual world. In addition, they allow for a comparison of the effectiveness of activities carried out in institutions beyond the scope of the "Education For Cybersecurity" project.

A total of 847 students representing a wide range of socioeconomic backgrounds from 14 different schools in Szczecin, Gdańsk, and Koszalin took part in the interviews. The age range of the participants in the discussions was 14 to 17 years, consisting of 402 boys (47.1%) and 445 girls (52.2%). The students were assured that their identities would remain anonymous and that the information would only be used for the purposes of this study.

The main objectives of this survey were, firstly, to diagnose the frequency of Internet use; secondly, to assess the prevalence of cyberbullying in the form of publishing malicious content on the Internet; and thirdly, to determine the degree of awareness among young people of preventive measures against cyberthreats and the possibility of receiving help in the event of cyberbullying. The rationale for carrying out this study was that students involved in cyberbullying are also involved in traditional bullying. Therefore, rather than viewing cyberbullying as a new phenomenon, it should be seen as an extension of traditional bullying. Furthermore, the relationship between cyberbullying and gender was investigated. The findings indicate that girls were more likely than boys to be victims and that boys were more likely to engage in cyberbullying. An examination of the relationship between gender and social support variables, such as friends, family, and others, showed that girls who were victims of cyberbullying reported having more support than boys. These findings can serve as a basis for prevention and intervention programs to deal with cyberbullying.

The issue of age is worth noting, as the older the participants were, the more distanced they were about participating in the conversation. The percentage of people who were reluctant to share their insights ranged from 5% to 7%.

The research revealed that the use of cybersecurity education programs positively influenced the degree of knowledge among respondents as to how to counter cyber threats. A correlation was also established between the knowledge provided and the degree of awareness among young people about seeking help in case of problems such as cyberbullying.

ISSN 2543-7585 e- ISSN 2543-8409

The project forces one to wonder if the same effect can be achieved without this mechanism. Based on a survey conducted among schoolchildren who were not included in the project, the level of awareness of cyber threats in 2021 was almost at the same level as in 2019. In addition, based on responses to anonymous online surveys, the phenomenon of cyberbullying is still experienced by students. The project thus provides an opportunity not only to implement preventive measures, but also to assess the effectiveness of such activities in cybersecurity education.

The case study in this area can verify the effectiveness of the project and, through its empirical nature, point to actions to strengthen existing incentive structures on the part of public entities. Knowledge of the mechanism of cooperation is crucial for the success of the project and its implementation requires knowledge of the nature and specificity of each of the participating parties to help in understanding the nature and cause of resistance to innovation in the public sector.

Such empirical knowledge gives this project of cybersecurity education a much stronger scientific basis. Thus, not only is there a need to monitor this phenomenon, but there is also a need to use benchmarking to evaluate the achievements of the project. This presents an opportunity for a more targeted approach to cyber threat prevention education in schools. A model of how teachers can react when unpleasant events occur in their daily work can also be developed. The support of the police and academic institutions is also an added advantage.

Survey Results, 2019–2021

Year 2019							
Questions	Do you have a computer with Internet access in your home?	Have cybersecurity classes been taught at your school?	How many hours a day do you spend in front of a computer?	Have you posted a ridiculing or violent picture/video/content about yourself online? (number of times recorded)	Have you sent a ridiculing photo/video/content ridiculing your friends?	Do you send pictures of yourself to friends you meet online?	Do you know who to turn to for help when you are faced with cyberbullying?
Schools covered by the program	92 - Yes	42 - No 47 - Yes 11 - I don't remember	4.5	6	4	7	Yes - 63 No - 37

Schools not included in the program	89 - Yes	64 - No 7 - Yes 29 - I don’t remember	4	5	5	9	Yes - 59 No - 41
Year 2020							
Questions	Do you have a computer with Internet access in your home?	Have cyber-security classes been taught at your school?	How many hours a day do you spend in front of a computer?	Have you posted a ridiculing or aggressive picture/video/content about yourself online?	Have you sent a ridiculing photo/video/con tent ridiculing your friends?	Do you send pictures of yourself to friends you meet online?	Do you know who to turn to for help when you are faced with cyber-bullying?
Schools covered by the program	90- Yes	38 - No 46 - Yes 16 - I don’t remember	5	12	0	1	Yes - 66 No - 34
Schools not included in the program	91- Yes	54 - No 15 - Yes 31 - I don’t remember	3	14	2	8	Yes - 62 No - 38
Year 2021							
Questions	Do you have a computer with Internet access in your home?	Have cyber-security classes been taught at your school?	How many hours a day do you spend in front of a computer?	Have you posted a ridiculing or aggressive picture/video/content about yourself online?	Have you sent a ridiculing photo/video/con tent ridiculing your friends?	Do you send pictures of yourself to friends you meet online?	Do you know who to turn to for help when you are faced with cyber-bullying?
Schools covered by the program	88- Yes	37 - No 50 -Yes 13 - I don’t remember	5	6	0	2	Yes - 72 No - 28
Schools not included in the program	92- Yes	46 - No 31 - Yes 23 - I don’t remember	4	13	4	6	Yes - 68 No - 32

The answers to the first question show that young people have no difficulty accessing the Internet, which may imply a greater risk from digital threats. There is also not much difference in the results between the schools in the program and those outside it.

The results in the second column show that young people from the participating schools tended to remember the program’s activities, but the progress was not as great as one might expect. The significant number of negative responses among this group of students is puzzling. It may be due to the very problem of remembering such events or giving answers out of spite. Obviously, it would be advisable to hold more frequent meetings with young people on a given subject. Despite this, however, there was a noticeable increase in awareness of cyber threats (particularly evident in the sixth column), which increased in the study group over the three-year period. The students in the non-participating schools also showed an upward trend in this area, but it was much weaker than in the participating schools.

Answers to the third question show that a large proportion of young people spend between 3 and 5 hours a day in front of a computer. Of course, the data refers to "active" computer use. However, access to the Internet itself, which is possible almost 24 hours a day through cell phone applications, for example, was not taken into account. This fact also forces us to reflect on another danger: young people becoming addicted to Internet communication.

The fourth point indicates an upward trend in the phenomenon of cyberbullying, which does not directly imply a lack of effectiveness of the project. The reported cases of cyberaggression prove that the cybersafety program must continue. In addition, the school environment is only one of many that can cause harm to a specific individual in the cyber world.

The results in the fifth column show the prevalence of cyberbullying in the study group. The problem did not appear in the answers from the schools covered by the program after the first year of it, which does not mean that the phenomenon no longer exists. Certainly, the results in the questionnaires do not perfectly reflect the reality, and the participation of the police in the program could have had an impact on this state of affairs. To sum up, it can be hypothesized that after having lessons with the police officer, who made the students aware of the legal consequences, none of the respondents wanted to admit to cyberaggression (despite the anonymity of the questionnaire), or, it can be optimistically assumed that they abandoned such activity. The problem, however, is evident in schools outside the cybersecurity education project.

The answers to the sixth question indicate the success of the project, as there is more awareness of the dangers of sending photos of oneself to strangers on the Internet or posting them on social networking sites. It should also be noted that there was also an improvement in this area – albeit slightly less of one – in the schools not included in the project.

The seventh point also indicates increased knowledge about cybersecurity. The awareness among the respondents about whom to contact in case of cyberbullying has clearly increased, with the difference being that this knowledge was more widespread in the schools covered by the program. On the other hand, it is worth noting that the level at baseline (i.e., in the 2019 survey) was already high, as more than half of the surveyed youths in both cases answered in the affirmative.

Analyzing an innovation is a major challenge for a researcher because it requires a meticulous approach to every aspect and a commitment of time to be able to discover the nature of the changes taking place. The experiment is costly and time-consuming for all concerned. The aim of this project was to determine the specific mechanism of cooperation between institutions responsible for cybersecurity, through observation and analysis of the information exchange between them. The project is pioneering for the area of cybersecurity education, which makes it difficult to implement. Until now, there have been signals at scientific conferences about the need for collaboration that, with the power of synergy, lead to much better results. The model of public cooperation in cybersecurity is difficult to implement in practice, due to the fact that, firstly, the implementation of this type of project is unknown to public entities, and secondly, it concerns a virtual space used by young people, who are a rather hermetic social group. Therefore, it is worth emphasizing that Internet users as well as cyberspace itself constitute a great research challenge for research in this field.

ISSN 2543-7585 e- ISSN 2543-8409

ISSN 2543-7585 e- ISSN 2543-8409

Conclusion

An awareness among the local community about cybersecurity and how to deal with cyber threats can help reduce the number crimes and victims. The project was a source of information for junior high school students, teachers, researchers, residents, officials, and uniformed services, which will have a unique opportunity to establish cooperation and exchange knowledge. This model also provides an opportunity, especially for young people, to develop a positive image of the police and an active attitude towards breaking the law. The cooperation program has the potential not only to improve cybersecurity, but can also be used to implement new ideas from other areas of public policy.

Cybersecurity research is an opportunity for innovation in the public sector. It also points to new opportunities for scientific engagement in the field of local government collaboration. The project "Education For Cybersecurity" is designed to make the local community aware of the dangers of using new technologies. The program also activates the local community, which can share their knowledge and needs in this area and, through scientists and the uniformed services, familiarize themselves with the problem of cyber threats. Future research should explore the links between cyberbullying and sociodemographic factors and parenting and caregiving styles. The study's findings suggest that prevention and intervention programs, which usually focus on helping victims of cyberbullying, should also include people who have clear social/emotional problems and may engage in cyberbullying to escape problems at home or school or other problems associated with growing up.

References

Cole, R. (1988). The public sector: The conflict between accountability and efficiency. *Australian Journal of Public Administration*, *47*(3), 223–232.

Cooke, P. (2017). "Digital tech" and the public sector: What new role after public funding? *European Planning Studies*, *25*(5), 739–754.

Domurat, I. (2012). He claimed to be a 12-year-old girl: Provocation on the Internet. *Głos Koszaliński*, *231*(1), 1.

Gillespie, A. A. (2016). Cybercrime: Key Issues and Debates. New York Routledge.

Holt, T. J. (Ed.). (2016). Cybercrime through an interdisciplinary lens. New York Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. (2015). Cybercrime and digital forensics: An introduction. New York Routledge.

Horbach, J., Oltrab, V., & Belinb, J. (2013). Determinants and specificities of eco innovations compared to other innovations: An econometric analysis for the French and German industry based on the community innovation survey. *Industry and Innovation*, *20*(6), 523–543.

Kearney, M., Schuck, S., & Burden, K. (2020). Digital pedagogies for future school education: Promoting inclusion. *Irish Educational Studies*, *41*(1), 117–133.

Kravariti, F., & Johnston, K. (2020). Talent management: A critical literature review and research agenda for public sector human resource management. *Public Management Review*, *22*(1), 75–95.

Lember, V., Kattel, R., & Kalvet, T. (2015). Quo vadis public procurement of innovation? *Innovation: The European Journal of Social Science Research*, *28*(3), 403–421.

Pillay, S. (2008). A cultural ecology of new public management. *International Review of Administrative Science*, *74*(3), 373–394.

Plamer, A. (1993). Performance measurement in local government. *Public Money & Management*, *13*(4), 31–36.

Potts, J., & Kastelle, T. (2020). Public sector innovation research: What's next? *Innovation: Management, Policy & Practice*, *12*(2), 122–137.

Sanina, A., Balashov, A., & Rubtcova, M. (2021). The socio-economic efficiency of digital government transformation. *International Journal of Public Administration*. https://doi.org/10.1080/01900692.2021.1988637

ISSN 2543-7585 e- ISSN 2543-8409

Sanina, A., Balashov, A., Rubtcova, M., & Satinsky, D. M. (2017). The effectiveness of communication channels in government and business communication. *Information Polity*, *22*(4), 251–266.

Schick, A. (1998). Why most developing countries should not try New Zealand's reforms. *The World Bank Research Observer*, *13*(1), 123–131.

Smith, R. (2016). Bureaucracy as Innovation. *Research-Technology Management*, *59*(1), 61–63.

Stawasz, E., & Nodbalska, G. (2011). Innovation dictionary, lexicon of keywords. PAN.

Toivonen, M., & Tuominen, T. (2009). Emergence of innovations in services. *The Service Industries Journal*, *29*(7), 887–902.

Torgal, C., Espelage, D. L., Polanin, J. R., Ingram, K. M., Robinson, L. E., Sheikh, A. J. El., & Valido, A. (2021). A meta-analysis of school-based cyberbullying prevention programs' impact on cyber-bystander behavior. *School Psychology Review*. https://doi.org/10.1080/2372966X.2021.1913037

Trček, D., & Likar, B. (2014). Driving information systems security through innovations: First indications. *Cybernetics and Systems: An International Journal*, *45*(1), 56–68.

Unceta, A., Luna, Á., Castro, J., & Wintjes, R. (2020). Social innovation regime: An integrated approach to measure social innovation. *European Planning Studies*, *28*(5), 906–924.

Wall, D. S., & Williams, M. (Eds.). (2014). Policing cybercrime: Networked and social media technologies and the challenges for policing. New York Routledge.

Webster, E. (2004). Firms' decisions to innovate and innovation routines. *Economics of Innovation and New Technology*, *13*(8), 733–745.

ISSN 2543-7585 e- ISSN 2543-8409