

Original article

Impact of threats from the use of modern information technologies on university students' learning outcomes. Part I

Mariusz Frączek* , Leszek Wolaniuk 

Faculty of Security Studies,

General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland,

e-mail: m.fraczek007@gmail.com; leszek.wolaniuk@awl.edu.pl

INFORMATION

Article history:

Submitted: 21 July 2020

Accepted: 16 November 2020

Published: 15 September 2021

ABSTRACT

The study presents theoretical assumptions of the research in the scope of the impact of threats resulting from the use of modern information technologies on students' education outcomes. Part I addresses the theoretical and methodological aspect of research conducted in 2019. It systematizes the considerations undertaken, their brief characteristics, and the course of research. The conclusions include ones drawn after the implementation of the initial stage and the theoretical part together with the adopted assumptions. Attention was drawn to the broad spectrum of the research area, which so far has not covered civilian students of a hierarchical university in terms of the negative impact of threats resulting from the use of modern information technologies.

KEYWORDS

modern information technologies, Internet, communication, threats

* Corresponding author



© 2021 by Author(s). This is an open access article under the Creative Commons Attribution International License (CC BY). <http://creativecommons.org/licenses/by/4.0/>

Introduction

The end of the second decade of the 21st century confirms the dynamic development of various modern information technologies and related services for interpersonal communication. A natural consequence of technological progress has also become the possibility of applying them to the dissemination of education and access to global information resources gathered on numerous servers and databases. The latter is particularly appreciated by young people, especially the generation that no longer knows and remembers their lives without Internet access. They are the ones who determine today which services and message delivery expectations will soon be of great importance. That applies both to the development of devices and dedicated software. The interconnection of computers and telecommunications into a single ICT network and the possibility of sharing data between all its users is regarded as a revolution in exchanging messages, and its natural consequence has been an avalanche of information transmission. That is facilitated by the progressive development of the IT infrastructure and ever-smaller size of communication devices, as well as tools created and

available to the individual recipient. The new IT and telecommunications solutions are undoubtedly characterized by numerous facilities for information collection and transmission. However, it is worth noting that they may also be a source of many threats, which will be further indicated. They cause an unconscious user to be exposed to dangers while using mobile telephone networks and the global network terminal equipment (desktop and mobile computers, including tablets, laptops, and notebooks). Risks to the use of modern information technologies also exist in the case of university education. That is since most young people have at least two devices enabling them to exchange information in a digitized form in various ways, while they are often unaware of the dangers of using the Internet primarily.

Research subject

As a primary indicator of their conduct, the authors have adopted the thesis that the priority task of modern organizations is the capability of collecting, processing, and transmitting information, no matter what their geographical location and character are, but to ensure their safety, regardless of the means and technical equipment used. In this context, the ability to access knowledge in a broad sense through modern information technologies should be seen as a significant research problem [1-6]. Indeed, knowledge and scientific facts are a fundamental attribute of the functioning of any university. Nonetheless, it is worth remembering that the global network and the information made available in it do not always contain knowledge that is useful during studies. Internet usage is also burdened with numerous threats characterized by the authors of the article and described in the literature. However, to date, no scientific studies address the impact of threats resulting from the use of modern information technologies on the education of civilian students in a hierarchical university.

The analysis of facts indicates that threats coming from the virtual world may affect young people's perception of reality and acquisition of knowledge about the surrounding world. If one considers that studies are the culmination of the current period of education, it is appropriate to assume that selected dangers associated with the use of modern information technologies may directly affect students. Today, the global network is a fundamental source of information for them, including the subjects on the curriculum. That stems from the widespread access to the Internet via various mobile devices.

The lecturers put much effort into bringing the methodology and effective ways of gaining knowledge closer to students, paying attention to the principle of viewership, as well as the importance of the possibility of contemporary utilization of numerous sources of knowledge that may impact the quality of learning and education. A group of academic lecturers recommends that their students should primarily use the resources of libraries and reading rooms, including digitized correctly verified specialist ones. It is also pointed out that the variety of teaching materials and the increasingly frequent electronic form of publications and studies displace traditional ways of collecting and processing knowledge independently. The foundations for acquiring knowledge during studies are classes conducted by academic teachers and the subject literature. An exception to this rule may be materials prepared according to their best knowledge by lecturers and made available on an e-learning platform. In the authors' opinion, the lectures direct students to obtain further knowledge on their own. It is also worth bearing in mind that the information currently obtained during academic classes is increasingly often recorded and independently collected by students in a digital form. Therefore, the authors' most significant concern is the individual ability to obtain and process information from the global network, which is needed in a given field of study, since it

requires expertise to assess its usefulness. The authors' analyses indicate that students take an uncritical approach to Internet content.

It is unequivocally clear from the above findings that the factor determining the research directions should also be the risks associated with the use of modern information technologies and their impact on the results of student education through the uncritical use of data available on the global network. Their basis is a scientifically justified forecast of the situation. The probability of the effects of adverse events related to threats from the Internet anticipated in the future serves this purpose. The above statement applies to many areas of social life, including the whole conglomerate of issues related to the need to provide university graduates with education at the highest possible level.

In the final stage of theoretical considerations, the research subject, in a very general sense, was selected threats to the use of modern information technologies, which imply assumptions of the probability of negative actions and events occurring during the students' acquisition of independent knowledge during their studies. Those activities result from hypothetical and real dangers, the identification and neutralization of which are more or less related to the functioning of the higher education system.

The achievements of contemporary theory and practice concerning threats from the global network and adverse effects of incidents of low awareness among its users, as well as the authors' direct observations concerning the uncritical use of modern technical solutions by young people require a reflection. It can be reduced to answering the question: Has the development of modern information technologies and access to the global network resources changed the way students acquire knowledge over the last dozen or so years?

The answer to the above question suggests that it should be preceded by a scientific forecast of potential threats that may significantly impact on the university graduates' education level.

Research objective

The research aimed to identify threats from the use of modern information technologies and their impact on the level of knowledge acquired through them. Their generation has become the basis for further work to answer the question: do modern information technologies support or disrupt the process of educating university students? As a result, it was assumed that today's students' knowledge is also greatly influenced by the possibility of quickly obtaining diverse information from the global computer network. Given the technical aspect, the convergence of services and technologies is of great importance, as modern communication devices combine features previously known from fixed and mobile telephony and computer networks. In turn, the purchase of selected mobile devices is limited only by price and market availability.

The research objective presented allows the presumption that generating a precise forecast of the nature of potential threats and their characteristics will require the use not only of the achievements of safety sciences, but also of technical sciences, broad inclusion of all the possible factors determining inquiries on the issues under consideration, and regarding several problems in terms of the achievements of modern forecasting.

In their previous publications, the authors of the study indicated selected criteria for the division of threats that may occur while using modern information technologies. Considering the above, it appeared necessary to list the essential dangers, without describing them in

detail, for their proper understanding as they may affect contemporary students. The following threats essential were included:

1. Attacks on equipment resources and networks, among them the best-known ones, e.g., viruses, worms, trojans, hacking, equipment theft [7-11], or blocking services. For students, it may mean the theft of teaching materials, their studies, and even finalized qualification papers for the first and second cycle studies.
2. Changes in the control of access to services and resources are the result of an attempt to defraud the fees for unblocking access to resources by installing a malicious ransomware application. That involves encrypting the disk of the user's computer and unblocking it only after paying the indicated financial amount.
3. Cybercrime is a threat that can only occur with using mis-designed software, which is against the law and ethics, resulting in an automatic change of data or theft of financial resources. Lack of computer security leads to, e.g., unauthorized use of computational resources for illegal trade in cryptocurrency.
4. Cyber-terrorism, which is the "convergence of cyberspace and terrorism. It refers to non-lethal attacks and threats against computers, computer networks, and the information stored therein to intimidate or coerce the government or society into political or social aims. To qualify an attack as cyberterrorism, it should result in violence against people or property or at least do enough harm to create fear" [12, p. 55-84]. It is a deliberate intimidation of global network users.
5. Identity theft on social networking sites or the impersonation of the relevant account holder. That may cause sending offensive correspondence from a given electronic device (computer/laptop/tablet), e.g., to the university lecturers' addresses.
6. Carelessness when using e-mail (the university's e-mail account), which may result in the loss of login and password, an unauthorized person's access to both the e-mail account and the virtual university. The threat is presented in point 5.
7. The use of electronic banking by generally accessible, often passwordless computer networks of the university, which are divided into three types of threats:
 - a) access to e-banking accounts, logging in to a fake bank website, fraudulent use of passwords and logins to accounts, and then making unauthorized transfers from them,
 - b) transfers of monetary assets, various ways and attempts to obtain a PIN, the owner's password and telephone number,
 - c) paying with contactless cards (one-off amount up to PLN 100), including money theft through specialized software available for mobile devices.

In the cases mentioned above, the loss of funds takes place each time.

8. Violence and harassment by creating attitudes that glorify violence or intolerable behaviour in society, while stalking should be understood as deliberate, malicious and cyclical solicitation, or even harassment that threatens someone's safety using primarily telephones and computers (offensive e-mails, videos, photos, drawings, rumours, and blackmail). The threat is intimidation or harassment of global network users.
9. Pornography, including the use of such websites through the computer networks of institutions and research units. It occurs if access to adult websites is not blocked by the administrators of the university-municipal network.

10. Data storage in the so-called “cloud”, which allows for quick access to own resources. The main disadvantage is that their users rarely wonders where their collected files are physically located and who else has actual access to them. Media examples of unauthorised access to such resources clearly indicate that the electronic files stored in them are not secure.
11. Addiction to mobile devices and their services, which, except for addiction to all kinds of stimulants, has been increasing for almost two decades, especially for young people, who are struggling with addiction to computers, mobile devices and the Internet, known as “infonism”. To date, tobacco and alcohol addiction has been cited. Currently, access to global network resources, electronic mail, and social networks is crucial for a significant student population. A large amount of time spent on the Internet can harm behaviour and functioning in the real world.
12. Alienating a person from a society. That is facilitated by a weak Internet user’s psyche and everyday problems that they cannot cope with. They are gradually being taken away from the environment, neglect responsibilities at work or school and towards their loved ones, and spend all time out of sleep in the virtual world.
13. Lowering the level of education. In the authors’ opinion, one of the negative effects of dependence on modern technological solutions is the progressive lowering of the level of education among young people who have started to study at universities. This is the case when their uncritical use of information taken from Google or Wikipedia (which, however, is not a source of reliable and scientifically proven information) leads to the collection of information which is untrue, scientifically unproven, often deceiving the reality, or containing inaccuracies.

Research problems

The main research problem is the answer to the question: *what is the impact of threats resulting from the use of modern information technologies on the university students’ learning outcomes?*

The above considerations give rise to two fundamental and, at the same time, inextricably linked, specific research problems, which can be expressed in the form of questions:

1. To what extent can contemporary threats resulting from the use of modern information technologies influence the university students’ learning outcomes?
2. What are the fundamental paradigms of education to prevent the effects of uncritical use of unverified information often presented as scientific facts?

Solving the research problems specified above requires defining and examining several detailed issues included in the questionnaire. It has been recognised that, when considered separately, they are characterised by a certain distinctiveness or specificity, while when viewed comprehensively, they constitute a structured, logical whole.

Providing precise answers to the questions contained in the questionnaire should be a solution to the main problem and enable the intended research objective to be achieved.

Working hypothesis

In the context of the research problems thus defined, the following working hypothesis was adopted: *The spectrum of possible threats from the use of modern information technologies*

is diverse, and diagnosing them will allow taking rational action to increase awareness of the dangers associated with the uncritical use of information acquired from the global network, while independently deepening knowledge by students.

Research methodology

The methodology was planned in the following order:

1. Clarification of the subject and objective of the research.
2. Clarification of the main research problem and working hypothesis.
3. Identification of research stages and their subject scope.
4. Indication of the time and spatial scope of the research and the respondent group.
5. Definition of research methods, techniques and tools adequately to the research conducted.
6. Carrying out theoretical and empirical research within the main stage.
7. Analysis and synthesis of research results.
8. Preparation of a report from the conducted research.

The following research methods were used during the research:

- theoretical methods (analysis, abstraction, comparison, synthesis, inference),
- logical methods (interpretation of results),
- practical methods (opinion and judgement examination by survey technique).

The research process aimed to verify the main research problem and the working hypothesis. Specific procedures and research methods were applied to obtain objective results of the work conducted. The research cycle was divided into three stages, identical with the main components of the scientific method [Cf. 13, p. 68-171; 14, p. 66-74; 15, p. 31], whose goal was precisely defined (Fig. 1). In the initial stage, knowledge concerning the subject of the research was gathered, which made it possible to specify the problem situation, the research objective, research problems, and working hypothesis and initially adopt research methods and techniques. The main stage included the verification of the adopted working hypothesis through comprehensive solving research problems specified in the initial stage. The research results were finally verified in the final stage, the summary of which is a report from the conducted research.

When striving to obtain reliable results of the conducted works, the results of research on the varied nature of potential threats perceived through the prism of the possibility of using certain technologies by university students, were applied. Conclusions from previous analyses and direct observations in the field of the authors' interests were also taken into account.

The entire research process required the use of various research methods acceptable in the security science community, which covered all research problems. In the works, the respondents' judgments and opinions were used. The methods used enabled a critical evaluation of the obtained results and had a significant impact on their final effects and the shape of the research report.

The research implementation allowed for positive verification of the working hypothesis. Many additional circumstances and factors were generated. They affected the obtained results of the considerations in the aspect of using modern information technologies and their impact on the students' education.

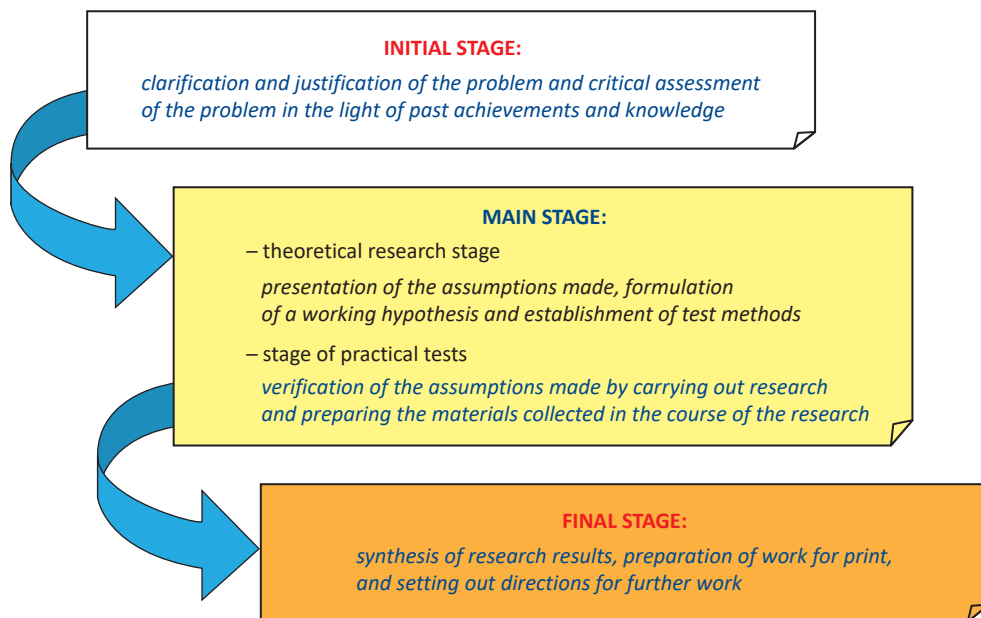


Fig. 1. Stages of the research process
Source: Own study.

The most important ones included:

- analysis of threats related to Internet access and modern information technologies and their impact on the youth,
- analysis of students’ learning outcome,
- compilation of the research results in the form of a report,
- conducting a survey of opinions and judgments,
- analysis of materials that directly and/or indirectly address the students’ ability to use modern information technologies.

The collected research material constituted the basis for generating conclusions, primarily in terms of how to act and inspire students to independently acquire the knowledge necessary for the implementation of the educational process in individual fields and levels of study.

The basis for conducting the research

To obtain reliable results, opinions and judgments were examined using a questionnaire survey, which was anonymously filled in by civilian students of the Military University of the Land Forces of National Security and Security Engineering faculties. The questionnaire form contained 17 questions, the first two of which were the respondents’ labels. The full content of the questionnaire questions, its analysis, and conclusions from it are presented in the second part of this publication.

Conclusion

The first part of the article presents the authors’ methodological workshop and the fundamental assumptions of the adopted empirical research, the results of which and their

discussion are included in the second part of the work. It should be emphasized that numerous factors can influence the results of student education. Therefore, it is not without reason that the basic division of risks to which young people gaining knowledge during their studies and any other person that, during their education, has not yet encountered the problem of safe use of modern information technologies, are exposed is presented. The research problems identified (the main problem and specific problems), the working hypothesis and the research methodology adopted constituted the basis for the implementation of empirical research and made it possible to verify it. The research methodology was presented alongside the methodological process. The authors focused their research only on the aspect of individual skills of using modern information technologies by students and their awareness of the resulting threats. They also do not refer to literature related to media didactics since in their scientific activity, they pay attention to information security and cyber threats. Neither have they analyzed the actions taken by persons responsible for the administration and security of the university's information and communication systems. It was assumed that they are protected under the applicable law and the requirements of a hierarchical organization. However, the account has been taken of the fact that modern mobile phone network operators offer a wide range of services related to access to data transmission, which means that civilian students can but do not have to use the access points in a given university.

The authors believe that Part I is a theoretical study that will allow for a full understanding of the practical research results presented in Part II and the final conclusions summarizing the entirety of the conducted considerations.

Acknowledgement

The study was created within the research project No. 127/NNB/51/DZS/2019. The work was financed by the Ministry of National Defense.

Conflict of interests

All authors declared no conflict of interests.


Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Mariusz Frączek  <https://orcid.org/0000-0002-2216-8053>

Leszek Wolaniuk  <https://orcid.org/0000-0003-0841-5684>

References

1. Bednarek J (sci. ed.). *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*. Warszawa: Difin; 2014.
2. Furmanek W. *Nowoczesne technologie w oświacie i edukacji*. *Edukacja – Technika – Informatyka*. 2014;5(2):15-26.
3. Furmanek W. *Dobra szkoła*. *Nowe Horyzonty Edukacji*. 2012;4(7).

4. Siemieniecki B. *Technologia informacyjna w polskiej szkole*. Toruń: Wyd. Adam Marszałek; 2004.
5. Tanaś M. *Media w edukacji*. Elektroniczny skrypt akademicki; 2010.
6. Tanaś M, Galanciak S (eds.). *Cyberprzestrzeń – człowiek – edukacja. T. 1. Cyfrowa przestrzeń kształcenia*. Warszawa: Oficyna Wydawnicza Impuls; 2015.
7. Frączek M. *Rola obrony cyberprzestrzeni dla funkcjonowania państwa i jego obywateli*. In: Frączek M, Marczyk M (eds.). *Wybrane aspekty bezpieczeństwa cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej*. Warszawa: Akademia Obrony Narodowej; 2014.
8. Frączek M. *Wpływ cyberprzestrzeni na funkcjonowanie systemu łączności wojsk lądowych – diagnoza problemu*. In: Kiezuń W, Wołeszo J, Pisarska A (sci. eds.). *Prakseologia w zarządzaniu i dowodzeniu. T. 1. Skuteczność w zarządzaniu*. Kalisz: Wydawnictwo Uczelniane Państwowej Wyższej Szkoły Zawodowej im. Prezydenta Stanisława Wojciechowskiego w Kaliszu; 2016, p. 135-46.
9. Jemioła T, Kisielnicki J, Rajchel K (eds.). *Cyberterrorizm – nowe wyzwania XXI wieku*. Warszawa: Wyższa Szkoła Informatyki, Zarządzania i Administracji; Szczytno: Wyższa Szkoła Policji; 2009.
10. Wolaniuk L. *Paradygmaty metodyki szkolenia wojskowego w kursach e-learningowych*. In: *E-learning a edukacja obronna*. Warszawa: Wydawnictwo Wojskowej Akademii Technicznej; In press.
11. Wolaniuk L. *Selected problems of security of information confidentiality in cyberspace*. Scientific Journal of the Military University of Land Forces. 2017;4(186):194-207.
12. Denning DE. *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa: Wydawnictwa Naukowo-Techniczne; 2002.
13. Kuc BR, Ścibiorek Z. *Zarys metodologii nauk o bezpieczeństwie*. Toruń: Wydawnictwo Adam Marszałek; 2018.
14. Maszke AW. *Metody i techniki badań pedagogicznych*. Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego; 2008.
15. Pieter J. *Z zagadnień pracy naukowej*. Wrocław: Wydawnictwo Zakładu Narodowego im. Ossolińskich; 1974.

Biographical note

Mariusz Frączek – Col., Dr. (hab.), Eng., Professor. The main area of his interests includes organization and operation of communication and IT systems, in particular, the possibilities of ensuring information protection and its safety in communication systems, ICT systems and networks, as well as in cyberspace. Moreover, the author also deals with the application of modern technologies in telecommunication and information technology. He is the author and co-author of publications in the organization, e-business, and protection of communication and IT systems and networks for defence and security needs, and the issue of possibilities of cooperation between the Armed Forces and uniformed services in crises.

Leszek Wolaniuk – Dr. Eng., Assistant Professor, Head of the Department of Security in Cyberspace at AWL. His area of interests includes computer science, cryptography, and safe application of modern technologies, including cyberspace. Author and co-author of publications in organization, operation, and protection of ICT networks used for security purposes.

Wpływ zagrożeń wynikających z użytkowania nowoczesnych technologii informacyjnych na wyniki kształcenia studentów w uczelni wyższej. Część I

STRESZCZENIE

W opracowaniu przedstawiono założenia teoretyczne badań w zakresie oddziaływania zagrożeń wynikających z stosowania nowoczesnych technologii informacyjnych na wyniki kształcenia studentów. Część I prezentuje aspekt teoretyczny oraz metodologiczny badań prowadzonych w 2019 roku. Dokonano usystematyzowania podjętych

rozważań, ich krótkiej charakterystyki oraz przebiegu badań. We wnioskach ujęto konkluzje powstałe po realizacji etapu wstępnego oraz części teoretycznej wraz z przyjętymi założeniami. Zwrócono uwagę na szerokie spektrum obszaru badawczego, którym dotychczas nie byli objęci studenci cywilni zhierarchizowanej uczelni wyższej w aspekcie negatywnego wpływu zagrożeń wynikających z użytkowania nowoczesnych technologii informacyjnych.

SŁOWA KLUCZOWE nowoczesne technologie informacyjne, Internet, komunikacja, zagrożenia

How to cite this paper

Frączek M, Wolaniuk L. *Impact of threats from the use of modern information technologies on university students' learning outcomes. Part I*. Scientific Journal of the Military University of Land Forces. 2021;53;3(201):454-63.

DOI: <http://dx.doi.org/10.5604/01.3001.0015.3398>



This work is licensed under the Creative Commons Attribution International License (CC BY).
<http://creativecommons.org/licenses/by/4.0/>