СОЦИОЛОГИЯ
SOCIOLOGY

Research Article
UDC 351-053.6(517.3)
DOI 10.18101/2949-1657-2024-2-3-12

INFORMATIONAL SECURITY, RISKS AND CONSEQUENCES OF DIGITALISATION AMONG MONGOLIAN YOUTH[1]

© **Khatanbold Oidov**[1]
(Ph.D),
Leading academic researcher
Institute of Philosophy
Mongolian Academy of Sciences
Ulaanbaatar, Mongolia
khatanboldo@mas.ac.mn

© **Tsetsenbileg Tseveen**[2]
(Ph.D),
Leading academic Researcher
Department of Sociology
Institute of Philosophy, Mongolian Academy of Science,
Associate Professor of Institute of Foreign Languages,
Peoples' Friendship University of Russia
Ulaanbaatar, Mongolia
tsetsenbilegts@gmail.com

Abstract. It is impossible to imagine the shape of the future of human society without the full functioning of communication, information exchange, daily financial transactions and the use of e-social services. However, rapid technological development brings threats and risks. Our aim is to identify measures for information security and to reveal the inherent risk of causing harm to young people through digitalization, their awareness, and their knowledge levels. In a 2022-2023 social study conducted by 800 young people in five provinces and the capital, Ulaanbaatar, it was found that young people did not sufficiently understand and understand the social risks of digitalization.
Keywords: Youth, Mongolia, digitalization, informational security, social risks, prevention

For citation
Khatanbold Oidov, Tsetsenbileg Tseveen. Informational Security, Risks and Consequences of Digitalisation Among Mongolian Youth. *Oriental Vector: History, Society, State.* 2024; 2: 3–12.

[1] The article was prepared with the support of a joint grant from the Science and Technology Foundation of Mongolia and the Belarusian Russian Foundation for Basic Research, SHUT 2022/01 — "Social risks of the youth of Belarus and Mongolia in the context of digitalization."

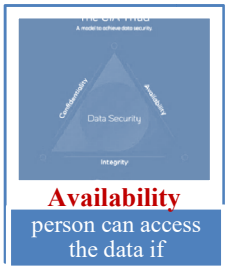
The 21st century has begun and continues with constant turbulence. Consequently, it is often associated with risks. Persistent conflicts, struggles and threats occur throughout the world. The Global Risk Report 2024 (November 19th) is a backdrop for rapid technological change and economic uncertainty and the world's two most dangerous crises: climate and conflict. It identifies four major risks influencing the realization and management of global risks over the next decade: climate change, demographic division, boundary technologies development pathways (technological acceleration) and geographic and strategic shifts.] (Global risks report, 2024) [The report warns of the effects of technological acceleration, such as misinformation and misinformation, and number one is the new leader of the top 10 rankings in the first year. The simple interface to large-scale artificial intelligence (AI) models, which no longer requires niche skills, has already enabled the explosion of falsified information and "synthetic" content, ranging from sophisticated voice clones to fake websites, such as paper, and clarifies the risks of digitalization, its consequences, and information security. Therefore, in the context of the above-mentioned topics, it seems appropriate to explain what information security is and how it should be implemented in our activities.

The rapid technological development, along with the undeniable advantages, presents threats and risks. The report clearly outlines and highlights the consequences: "Synthetic content will manipulate individuals, harm economies and fracture societies in many ways over the next two years. False information can be used to pursue various objectives, from climate action to escalation of conflicts. New types of crimes will also be abundant, such as inconsistencies in false pornography and stock market manipulation. However, even if the irrational spread of lies and lies threatens society's cohesion, some governments may act too slowly, thereby compromising the balance between the prevention of lies and the protection of freedom of expression, while oppressive governments may use stronger regulatory controls to undermine human rights.

Information security refers to a process and methodology designed and implemented to protect printing, electronic or other forms of confidential, private, sensitive information or data from access, use, abuse, disclosure, destruction, modification or damage caused by unauthorized access, misuse or disclosure [(Institute, 2016)]. Information is electronic, printed and other forms of information, and no matter how sensitive, secure and data-related, these elements mean that they cover all issues, in fact, these elements represent the most widely recognized "triads" of information security [(Security, 2023)].

In other words, information security is the three basic pillars of directing the productivity of any organization. It is understood that the following things, including a coherent structured risk management act in the process, will be revealed in order to avoid the seeds of policy in the implementation-focusing event. Specifically, (i) identify unexpected threats, vulnerabilities, and effects on information and related assets; (ii) identify, reduce, share, resolve risk in risk assessment procedures; (iii) identify, develop, and implement appropriate security measures when appropriate risk mitigation is required.

This is a part of management of risk information and often in data unauthorized unauthorised unsuitable treatment and access to the law otherwise use, disclosure, violation, destruction, corruption, use and falsification enter, check, register, reduce the degree of action in advance, including preventive content. Basically, it covers activities aimed at reducing the above-mentioned negative impacts.



In connection with the above-mentioned content, the problem of information security ("infosec")[(Curry Michael, Marshall Byron, Crossler Robert E, & other, 2018, pp. 49-66)] or practical approaches to information protection reduce information risk are discussed. Protection information may be electronic, physical (e.g. documents) or intangible (knowledge). It is part of information risk management [(Oshi Chanchala, Singh Umesh Kumar, 2017, pp. 128-137)] and usually includes the prevention of unauthorized access to data, unauthorized use, disclosure, violations, destruction, damage and use, fraud, verification, recording and data degradation. In short, it includes activities aimed at reducing the negative impacts of the above.

To standardize the field, researchers and practitioners collaborate to propose various industry guidelines, policies and standards for passwords, antivirus software, encryption software, legal responsibility, security awareness and training. These standards are supported by dozens of laws and regulations affecting data access, processing, storage, transmission and disposal. Furthermore, the implementation of any standard or guideline will likely have limited efficacy unless it promotes continuous improvement and compliance culture. For example, in the 1992 and 2002 revisions of the Guidelines for Information and Network Security by the European Economic Cooperation and Development Organization (OECD), there are awareness, responsibility, response, ethics, democracy, risk assessment, and security. It proposes nine generally accepted design principles, their implementation and security management. In addition, NIST's 33 principles [(Stoneburner G, Hayden C, Feringa A, 2004)] for information technology security were proposed as additional recommendations based on the above-mentioned principles in 2004.

From a security point of view, privacy is defined as *"no disclosure or disclosure of information to individuals or entities without legal permission"* [(K.Beckers, 2015, p. 100)]. In simple words, it is the component of privacy we implement to protect our data from anyone who uses it without our consent. The most common examples of electronic data infringements are laptop theft, stolen login passwords, or emails sent to the wrong person.

As far as data integrity is concerned, it involves maintaining the accuracy and integrity of data throughout its life cycle and ensuring it, which means that data cannot be modified without authorizing or discovering [(I.Hryshko, 2020, pp. 180-184)]. It is not the completeness of large databases' links, but the guarantee of information data (atomicity, coherence, isolation, durability) based on the ACID* model can be understood only for data transmission and processing. Information security systems usually include controls to ensure their security, particularly core and essential functions, against

deliberate and accidental threats. In broad terms, data security encompasses human-social relationships and processes, business integrity, and data security principles.

Information availability: All information systems must be easily accessible if necessary to achieve their objectives. This means that some communication channels must work properly, including computer systems used to store and process information and security measures used to protect it [(Video from SPIE, 2021)]. High-availability information systems can prevent power outages, equipment failures, system upgrades, and service interruptions.

Information security risks have dozens of possibilities. For example, attacks on IT software, theft of intellectual property, identity theft, theft of equipment and data, sabotage and data extortion should be mentioned. Furthermore, the theft of intellectual property still brings significant losses to companies in the information technology sector. In addition, identity theft has become a common practice of theft of basic information by accessing an individual's basic information through social engineering. Moreover, the widespread use of mobile devices has increased the volume of personal data in recent years, and cybercriminals using information technology, such as stealing, destroying and disseminating personal information, have become an important challenge in electronic development. There are many ways to protect yourself from these attacks, but the most important is to prevent cyber attacks. One of them is to provide information regularly to this user. To do this, you can reduce risk by creating and updating a multi-layer security software regularly. In addition, to mitigate the risk of outsourcing to corporate information, we constantly increase the costs and value of information technology, establish permanent mobile control systems, such as information distribution, distribution, and transmission through monitoring. Moreover, the assessment of potential losses arising from information threats and the development and implementation of risk response plans are the basis for preventing the above risks.

On the other hand, the use of digital environments, the process of influencing others through them, and rapid change of ideas create a single evolution that makes society as a whole too dependent on the online world. This has caused problems and risks for us. For example, science has not yet measured and studied the actual role of the Internet in today's politics. Furthermore, threats from ideology extremism, terrorism and cyberspace continue to have a negative impact on the security of all countries. We also need time to study scientifically how to protect ourselves from threats and avoid risks. Mass demonstrations through the media and social media are an obvious example of this, and the necessary changes in public consciousness and thought are needed to take and implement important measures to define society's real image and imagination.

The rapid growth of the Internet is the basis for young people who are influenced, involved in their activities, appreciate and support some extremist organizations, falling under their influence. The need to restrict, control and discover positive and negative trends has become the most important task of the national social security agencies, scientific institutions and research organisations. In particular, the establishment of a network group for public discussion of social problems will promote the special contribution of the Internet environment. In such cases, this form of communication is expressed through public organizations, street strikes and demonstrations. The Internet community therefore uses it as a user-friendly tool for planning and organizing real events.

In a 2022 national study conducted in Mongolia, young people were asked how they knew of cybersecurity threats. As a result, 65.3% of young people are aware of the risks of the Internet, 60.3% are aware of computer viruses, 61% are aware of forged information, 51.1 percent are addicted to the Internet, and 51.5 percent are aware of fraud and cyber theft. Meanwhile, 35.9 percent of the young people surveyed responded that they had heard about information-management of human consciousness and behavior (Table 1).

Table 1. Knowledge related to electronic risk
(1-knowledge, 2-knowledge, 3-not know)

№	Related risks	Known	Heard	DK	Average meaning
1	Computer virus	65.3	24.1	10.6	**1.5**
2	Internet addiction	59.1	28.6	12.3	**1.5**
3	Information warfare	38.8	32.1	29.1	**1.9**
4	False information	61.0	25.9	13.1	**1.5**
5	Confidential testimony	29.5	33.3	37.3	**2.1**
6	Electronic theft and fraud	51.5	34.8	13.8	**1.6**
7	The manipulation of human consciousness and behaviour by information.	36.5	35.9	27.6	**1.9**
8	Right to privacy	43.1	34.9	22.0	**1.8**
9	Right to protection of reputation	49.3	28.5	22.3	**1.7**
	Total				**1.7**

Note: The numerical average is measured on the scale (1 very bad, 2 bad, 3 moderate, 4 good, 5 excellent).

Since the digitalization of the information age, the risk among young people aged 18 to 32 is believed to have increased in rural areas as a result of urbanization.

If the risk of digitalization is calculated by the percentage of urban and rural populations, the following situation is observed (Table 2).

Table 2. Percentage of digital risk awareness

№	Zone	Knowledgeable	Knowledgeable Average	Ignorant
1	Urban area	37.1%	32.7%	30.3%
2	Rural area	29.2%	35.9%	34.9%

Source: The Social Risks of Youth in the Digital Age. Ulaanbaatar Park. NUM, UB., 2023.

From the above explanation, since the urban and rural population ratios are different, comparisons are not appropriate. However, to know how the effects of digitalization differ between urban and rural areas, knowledge levels must be determined. Compared to urban and rural youth, urban youth know the positive and negative aspects of digitalization, but lack knowledge of how to avoid them. According to the survey,

30.3% of youth are unaware of this. And (ii) rural young people are opposite to the above, i.e. 34.9% of young people are unaware.

The comparison of young people with digitalisation risks according to their level of education:

Table 3. Comparison of knowledge indexes with the education status of young people (percentage)

№	Level of Education	Knowledgeable	Knowledgeable Average	Ignorant
1	Uneducated	25.0	0.0	75.0
2	Primary education	20.0	20.0	60.0
3	Incomplete environment	30.0	50.0	20.0
4	Secondary school	30.3	38.9	30.8
5	Special environment	28.3	38.3	33.3
6	Higher /Bachelor's degree/	37.5	30.2	32.2
7	Master's degree	29.3	39.0	31.7

Source: The Social Risks of Youth in the Digital Age. Ulaanbaatar Park. NUM, UB., 2023.

As shown in the figures, 75% of young people with primary or low education levels do not know enough about the impact of social influences. Meanwhile, young people with incomplete secondary and secondary specialized education have a moderate knowledge of the negative effects of the social environment. It can be concluded that young people with bachelor's degrees have relatively good knowledge in this regard.

For example, the above results show that people are familiar with e-risks and hear them, but that they are relatively weak in terms of realization. Furthermore, the above table and the results of qualitative analyses show that young people have low level knowledge of the electronic environment. As some youth representatives have pointed out, they do not have sufficient knowledge of electronic risk, do not have experience with electronic risk protection, and behave as if they were not exposed to electronic risk.

The lack of knowledge about the security of personal data. Knowing there are privacy settings, but not knowing how to use them. There is insufficient action to use it in the public and there is no specific action to use it.

Government policy and measures are not being taken to protect and prevent cyberrisks. Cyberattacks are now common. With the increase in the use of the Internet, the mode of operation of offences has declined, resulting in more and more cyber attacks against teenagers and young boys.

Another important result of digitalisation for young people is the security problem. Information security is particularly the most dangerous result of the youth survey, as shown in the following figures.

In order to protect your reputation, you need to protect your personal information. For example, young people know that they do not share passwords and codes for bank-

ing and Internet services, including personal information, with others. Young people are very cautious about protecting their personal information and using any necessary means to protect their reputation in the online world, and it is observed.

However, young people pointed out that the consequences of crime are the next major consequences of digitalization. In particular, the fact that cybercrime victims have become increasingly frequent in recent years. In addition, teenagers tend to "hijack" them through online news and information, emotionally damage, harass and threaten, and they can see their negative or abnormal behavior in the following diagram.

The respondents know more about information security measures: "Do not share passwords or codes with anyone (including banks and the Internet)," "Secure personal information to protect your reputation", and "use the Internet for educational purposes".

These implications clarify that social risks faced by young people are characterized by diversity and interdependence. Education, education, economy and leisure are among the most important social risks associated with digitalisation. Of the 18 to 32-year-olds surveyed, 36.8% or the majority heard about privacy protection settings, but did not know how to set them up and use them as actions. Every day. Therefore, in the age of widespread use of social media, the measures for sharing information and protecting privacy among young people are inadequate, and despite rumours of the effects of digitalization, knowledge remains lacking.

One of the most common consequences is that information published in the media affects people's thoughts and behaviours. Analyzing the results of qualitative research has revealed the following picture. Specifically:

Many consequences of digitalization have a major risk. However, there is one. Cyber risk is normal. At least for the young daughter of a family member. The teenager's profile includes several unrecognized anime pictures. There are also animated teens who cheat.

I don't know much about the personalization of my online account. Personalized mobile data devices. iPhone and Samsung users are familiar with this customization, but are rare. Teens exposed to cybercrime are more likely to develop depression, depression and suicide tendencies.

Fraud using mobile phones is a common phenomenon. In particular, frequently recorded offences include the use of stolen telephones via telephone codes to attack user personal information, sending false messages to contacts, family members, and close friends, transferring money fraudulently to accounts, and then selling phones for spare parts.

The above-mentioned analysis shows that digitalization has a major negative impact, and quantitative and qualitative studies show that the Internet has a direct impact on human behavior. Therefore, matrix methods are used to test the level of awareness

of the possible consequences of Internet use. As a result, large-scale risks may increase.

The number of cyberattacks by external and Koi logging has increased considerably in recent years. The majority of these attacks took place last year using coins. Friends of Coin founded the crime, and online money disappeared without trace, eventually no one was prosecuted, and people who wanted to get rich were exposed to the risk of electronic money being "like a stone falling into the water".	

Among 18-32-year-olds participating in a survey on the social risks posed by digitalization, 34% are “very common”, 28.5 percent are “widespread”, 29.1 percent are “moderate”, 7.3 percent are. "No", while 1.1 per cent replied "no". While some of the risks associated with the use and use of the Internet are now increasing dramatically, among 18-32-year-olds in our current survey, the following risks are not only caused by digitalization, but are also common: the risks of the future.

According to the study in this context, the Government has developed and implemented specific targets for young people, but in real life, for example, it is not possible to implement them as a genuine reflection. In this context, participants from the 18 to 32 years of age in the study were explained and their views on the programme and activities to be implemented are as follows.

According to a survey, 24.4% of young people do not know much about government programmes and activities for young people. 8.6% of respondents believed that more youth psychological centres and places to spend their free time needed to be increased. In addition, 7.2 percent emphasized the need for public participation to organize events, 6.7 percent to listen to young people and involve them in the workplace, and 6.6 percent to organize thematic trainings.

Young people involved in the study stressed the need to take the following measures to reduce the social risks posed by digitalization. For example, it is considered to reduce Internet use (8.8%), not to disclose personal information (7.8%), and to control Internet use (5.8%). Furthermore, 12.5% of young people did not know about cyber risks, while 27.5 percent thought there were no risks in cyber environments. Qualitative analysis shows the following interesting results.

For example, proper use at all levels is essential, e-culture is developed, people will not establish a relationship without knowing someone, and will ultimately become victims of e-crime, and e-moral education is provided at all levels. Education institutions and families. Furthermore, the dissemination of electronic advertising and public comment on all risks associated with digitalization. In addition, the results of the study show that individuals must take responsibility for all the risks posed by digitalization and create an appropriate legal environment for the prevention and punishment of cybercrime in accordance with law and regulations.

Conclusion

This paper aims to uncover the hidden risks to the daily life of young people caused by digitalization and analyze the risks to find ways to prevent them. Consequently, it has been found that there is insufficient understanding and representation of the social

risks of digitalization in young people. The results of the study show that social risks are usually preventable, while people understand the need to find ways to prevent economic and natural risks.

This paper aims to identify hidden risks to young people's daily lives caused by digitalization and analyze them in order to find ways to prevent them. As a result, it has been found that young people do not understand and express sufficiently the social risks posed by digitalization. The research revealed that social risks are usually preventable and that people understand the need to find ways to prevent economic and natural risks.

If the standards for individual space and rights in electronic society are legalized and converted into legal standards, they may become far from human thought, thereby making it difficult for people to understand. Only understanding the meaning of human life, consciously understanding the norms of a just life, and providing intellectual ability to follow them are the challenges of today's increasingly mobile Internet use. Human history has shown that the blocking of things and the excessive control of things can have negative consequences. Likewise, in today's digital world, the risk of cyberattacks and crime will decrease and increase. Young people of the new generation must be adequately involved in the Internet environment to prevent e-risk, learn and use different information technology settings to protect e-safety, and have relatively high information on e-safety. Electronic information technology.

Bibliography

Institute, S. (2016). *Sans.org*. Retrieved from https://www.sans.org/information-security/

Security, D. (2023, October 24). *What are the 3 Components of Information Security? (CIA Triad)*. Retrieved from https://dotsecurity.com/insights/blog-what-are-the-components-information-security

Oshi Chanchala, Singh Umesh Kumar. (2017). Information security risks management framework — A step towards mitigating security risks in university network . *Journal of Information Security and Applications, 35* (doi:10.1016/j.jisa.2017.0), 128-137.

Curry Michael, Marshall Byron, Crossler Robert E, & other. (2018, April 2015). InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior. 49-66. Retrieved from doi:10.1145/3210530.3210535; 49 (SI): 49–66.

Stoneburner G, Hayden C, Feringa A. (2004). *Engineering Principles for Information Technology Security (PDF)*. Retrieved August 2011, from csrc.nist.gov. doi:10.6028/NIST.SP.800-27rA.

K.Beckers. (2015). *Pattern and Security Requirements: Engineering-Based Establishment of Security Standards.* Springer. ISBN 9783319166643.

I.Hryshko. (2020). Unauthorized Occupation of Land and Unauthorized Construction: Concepts and Types of Tactical Means of Investigation I(43): 180–184. *nternational Humanitarian University Herald. Jurisprudence*(43), 180-184.

Video from SPIE. (2021, May 29). the International Society for Optics and Photonics. Retrieved from doi:10.1117/12.2266326.5459349132001.

Global risks report. (2024). Retrieved from World Economic Forum: https://www.weforum.org/publications/global-risks-report-2024/

The article was submitted 07.06.2024; approved after review 11.06.2024; accepted for publication 13.06.2024.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, РИСКИ И ПОСЛЕДСТВИЯ ЦИФРОВИЗАЦИИ СРЕДИ МОЛОДЕЖИ В МОНГОЛИИ

Хатанболд Ойдов
Ph.D, ведущий научный сотрудник,
Институт философии
khatanboldo@mas.ac.mn

Цэцэнбилэг Цэвээн
Ph.D, ведущий научный сотрудник,
Институт философии;
доцент,
Российский Университет Дружбы Народов
tsetsenbilegts@gmail.com
Монгольская Академия Наук
1 Амариин Гудамж ул., 210620 Улан-Батор, Монголия

Аннотация. Невозможно представить будущее человеческого общества без полноценного функционирования коммуникаций, обмена информацией, повседневных финансовых операций и использования электронных социальных услуг. Однако стремительное технологическое развитие приносит угрозы и риски. Наша цель — выявить меры по обеспечению информационной безопасности и раскрыть присущие риски нанесения вреда молодежи через цифровизацию, их осведомленность и уровень знаний. В ходе социального исследования, проведенного в 2022–2023 гг. среди 800 молодых людей в пяти провинциях и столице Улан-Баторе, было установлено, что молодежь недостаточно понимает социальные риски цифровизации.
Ключевые слова: молодежь, Монголия, цифровизация, информационная безопасность, социальные риски, профилактика.

Для цитирования
Оидов Хатанболд, Цэвээн Цэцэнбилэг. Информационная безопасность, риски и последствия цифровизации среди молодежи в Монголии // Восточный вектор: история, общество, государство. 2024. Вып. 2. С. 3–12.

Статья поступила в редакцию 07.06.2024; одобрена после рецензирования 11.06.2024; принята к публикации 13.06.2024.