THE UNSEEN ENEMY: A SCIENTIFIC EXPLORATION OF DIGITAL RISKS, IMPLICATIONS OF DIGITAL RISKS, THREATS, AND SCAMS ON USERS' WELLBEING

Umurzoqov Mexroj Umar o`g`li
E-mail: umirzakovm7@gmail.com
Ministry of Foreign Affairs of the Republic of Uzbekistan University of World Economy and Diplomacy, Graduate Student of the Faculty of International Law

Abstract: The main objectives of the article, the concept of digital risks, their types, the causes they cause, methods of Prevention, statistics and expert opinions on this area are summarized. Introduce the significance of the study in the context of the modern IT-driven world. Define digital risk and highlight the importance of understanding its implications on users' well being. Briefly mention the experts and sources contributing to the definition of digital risk.

Keywords: Digital risk, Cybersecurity, Displaced populations, Process automation, Decision automation, Digitized monitoring, Cyber threats, Cloud technology, Data leaks, Workforce talent, Compliance risk, Resilience risk, Third-party risk, Data privacy, Digital risk protection, Proactive approach, Digital footprinting, Continuous monitoring, Threat intelligence.

Аннотация: Кратко излагаются основные цели статьи, понятие цифровых рисков, их виды, причины, которые они вызывают, методы предотвращения, статистика и мнения экспертов в этой области. Представьте значимость исследования в контексте современного мира, управляемого информационными технологиями. Дайте определение цифровому риску и подчеркните важность понимания его последствий для благополучия пользователей. Кратко упомяните экспертов и источники, которые внесли свой вклад в определение цифрового риска.

Ключевые слова: Цифровой риск, кибербезопасность, Перемещенное население, Автоматизация процессов, Автоматизация принятия решений, Цифровой мониторинг, Киберугрозы, Облачные технологии, Утечки данных, Талант рабочей силы, риск соответствия требованиям, Риск устойчивости, риск третьих лиц, Конфиденциальность данных, Защита от цифровых рисков, Проактивный подход, Цифровой отпечаток, Непрерывный мониторинг, Анализ угроз.

Abstract: Maqolaning asosiy vazifalari, raqamli xavflar tushunchasi, ularning turlari, sabablari, oldini olish usullari, statistika va ushbu soha bo'yicha ekspert xulosalari umumlashtirildi. Shuningdek, tadqiqotning ahamiyatini zamonaviy IT-boshqariladigan dunyo kontekstida tanishtirish. Raqamli xavfni aniqlash va uning

foydalanuvchilarning farovonligiga ta'sirini tushunish muhimligini ta'kidlangan. Raqamli xavfni aniqlashga hissa qo'shadigan mutaxassislar va manbalarni qisqacha eslatib o'ting.

Kalit so'zlar: raqamli xavf, kiberxavfsizlik, kiberhujum, jarayonlarni avtomatlashtirish, qarorlarni avtomatlashtirish, raqamlashtirilgan monitoring, kiber tahdidlar, raqamli texnologiyalar, muvofiqlik xavfi, chidamlilik xavfi, uchinchi tomon xavfi, ma'lumotlar maxfiyligi, raqamli xavfni himoya qilish, proaktiv yondashuv, raqamli izlar, doimiy monitoring.

Nowadays, we live in an enhanced world of IT, and it is very difficult to imagine our life without digital technology. Digitization processes bring numerous advantages to people, as well as various threats. Before delving into the risks posed by digital processes, it is crucial to define what digital risk is. Many experts in scientific articles give different opinions about this concept and the most common one is given from By Saptarshi Ganguly, Holger Harreis, Ben Margolis, and Kayvaun Rowshankish.

Digital risk is a term encompassing all digital enablements that enhance risk effectiveness and efficiency, especially process automation, decision automation, and digitized monitoring and early warning. The approach uses work-flow automation, optical-character recognition, advanced analytics (including machine learning and artificial intelligence), and new data sources, as well as the application of robotics to processes and interfaces. Essentially, digital risk implies a concerted adjustment of processes, data, analytics and IT, and the overall organizational setup, including talent and culture[1].

Cybersecurity Writer Edward Kost said that Digital risk refers to all unexpected consequences that result from digital transformation and disrupt the achievement of business objectives.

When a business scales, its attack surface expands, increasing exposure to cyber threats.This makes digital risk an unavoidable by-product of digital transformation and the advancement of new technology. Fortunately, strategies for digital risk protection have been developed to mitigate digital risks, enabling organizations to confidently scale their operations[2].

Digital risk is a growing concern, especially for displaced populations that often encounter unique barriers to accessing digital services and who may be particularly

[1] **Digital risk: Transforming risk management for the 2020s.** February 10, 2017 | Article. **By Saptarshi Ganguly, Holger Harreis, Ben Margolis, and Kayvaun Rowshankish. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s**

[2] What is Digital Risk? Definition and Protection Tactics for 2023. Cybersecurity Writer Edward Kost. https://www.upguard.com/blog/digital-risk#:~:text=Digital%20risk%20refers%20to%20all,its%20exposure%20to%20cyber%20threats.

vulnerable to cyberthreats and cybercrime when working in the digital economy. This Learning Lab session will explore the risks faced by displaced populations when engaging with digital services or jobs and livelihoods in the digital economy. It will consider how these digital risks can be defined, categorised and assessed in order to identify the most effective means to prevent and mitigate them. Digital risk is a broad and growing area of concern for researchers, technologists, and policymakers. However, humanitarian and development practitioners and their partners often lack guidance when it comes to understanding and addressing the various ways in which digital risk manifests for displaced populations. Forcibly displaced and stateless populations face a number of barriers to accessing digital services, upskilling opportunities, jobs and livelihoods that are mediated by digital technology and the platform economy. The gaps in legal, financial and social context may make refugees particularly vulnerable to cyberthreats and cybercrime when working in the digital economy. For example, many platformised labour opportunities require proof of identification, a bank account, or the right to work – access to which is not always easy for displaced populations. Additionally, the harms that can arise from using digital services – such as exposure to misinformation, lack of privacy, or potential for scamming – can have a disproportionate impact on those with fewer financial resources or those at greater risk of persecution. A framework for assessing the digital risks faced by forcibly displaced populations, and the harms they can engender, can equip UN agencies and their implementing partners with the tools to: identify sources of potential risk; work with governments, communities, communications providers, and technology companies to address them; and support forcibly displaced populations with safely navigating online services and the opportunities brought about by the platform economy. In an era where the gig economy, mediated by digital platforms, is providing increased opportunities to forcibly displaced and stateless populations, examining the risks that can arise from this engagement is crucial. While the gig economy may offer work opportunities to populations otherwise excluded from the formal labour market, it has often been shown to have the potential to increase financial precarity, create stressful conditions due to ‘algorithmic management’, and offer poor levels of protection from physical risks (such as accidents associated with platform-based delivery services). This Learning Lab will delve into what ‘digital risk’ means for displaced populations, as well as how it manifests in the context of gig work and the digital economy, in order to support UN agencies and their partners with promoting safe and fair use of digital services and technology for work and livelihoods.

Maximizing market research reports the following indicator:

Types of Digital Risk: The complexity of the digital risk landscape can be simplified by segmenting risks into different categories. Digital risk is comprised of nine primary categories, including:

1. **Cybersecurity risk.** This refers to the potential for unauthorised access, disruption or malicious activities targeting digital assets, systems or networks. It emphasises threats like malware, phishing and cyberattacks that can compromise data and infrastructure.
2. **Cloud Technology risk.** Pertains to vulnerabilities associated with storing data and running applications on remote servers. Risks include potential service outages, data breaches and reduced control over proprietary data.
3. **Data Leaks risk.** Involves the unintentional exposure of sensitive or confidential information, either internally or externally. Such leaks can result from weak security measures, human errors or system malfunctions.
4. **Workforce talent risk.** Centres on the challenges in attracting, retaining and training skilled personnel in the digital domain. A lack of qualified professionals can lead to operational inefficiencies and increased vulnerabilities.
5. **Compliance risk.** Relates to potential legal penalties and reputational damage from failing to adhere to regulatory requirements in the digital realm. Non-compliance can lead to fines, sanctions and loss of trust.
6. **Resilience risk.** Focuses on an organisation's ability to anticipate, respond to, and recover from adverse cyberevents. A lack of resilience can lead to prolonged downtimes, operational disruptions and reputational damage.

7. **Process automation risk.** Concerns about the challenges and vulnerabilities of automating digital processes. These risks include software bugs, system failures or unintended consequences of automation on business operations.
8. **Third-party risk.** Relates to the potential vulnerabilities introduced by external partners, vendors or suppliers. If these third parties lack adequate security measures, they can become weak links in an organisation's defence chain.
9. **Data privacy risk.** Involves potential threats to the privacy of individuals' personal data. This stems from unauthorised access, data misuse or non-compliance with data protection regulations.

The Internet Security Alliance provides the following information on cybersecurity risk:

• THE BAD NEWS: You can't "solve" the cyber security problem;

• THE GOOD NEWS: You can manage your cyber risk;

• Think of cyber as you think of your personal health…no one lives germ free[3].

No matter how you look at the issue, the advantage is on the side of the vandals-criminals, says expert Larry Clinton. Laws are lax. There are few experts who know the field. Attacks are easy and cheap to organize. The one who can do it will get a big reward.

Digital Risk Protection: Digital risk protection is a set of practices and methodologies to safeguard an organisation's digital infrastructure against ever-increasing digital threats. Digital risk protection solutions operate on the premise that organisations can use cybercriminal activity to their advantage to identify attacks before they happen.

There are several forms of digital risk protection (DRP), including:

- **Cybersecurity strategies:** Cybersecurity strategies must shift to a proactive, people-centric approach to protection. This is key to supporting ecosystem expansion while mitigating risk. Mitigating cyberattack risks is a critical part of DRP efforts.
- **Digital footprinting:** Digital footprinting involves discovering and mapping all digital assets exposed to potential threats. It is a critical part of digital risk protection and security awareness efforts.

[3] Internet Security Alliance. https://chapters.acp-international.com/images/newyorkcitymetro/ACO_NY_Metro-7-19-17.pdf;

- **Continuous monitoring:** Continuous monitoring of the security state of all exposed assets is essential to mitigate digital risk. This includes monitoring for vulnerabilities, threats and attacks.
- **Threat intelligence:** Threat intelligence solutions focus on improving security postures to help organisations withstand cyberattack attempts. They provide actionable insights into the latest threats and vulnerabilities.
- **Digital risk protection service:** Organisations with a complex digital landscape will achieve greater financial efficiency by investing in a digital risk protection service, often called DRPS. A DRPS is a comprehensive managed service that typically offers a platform, system or other technology to spearhead cybersecurity threat prevention.
- **Multidimensional threat analysis:** DRP solutions translate millions of data points into actionable business intelligence using multidimensional threat analysis, digital footprint contextualisation and threat evolution tracking.
- **Sensitive data leakage monitoring:** DRP solutions can monitor for sensitive data leakage, a valuable way for cybercriminals to exploit systems.

By implementing these forms of digital risk protection organisations can mitigate digital risk and confidently embrace the digital transformation necessary to scale in a fast-paced era[4].

When we talk about Cyber crime, we should attend to its classification in law. Cybercrime is defined as crimes committed on the internet using the computer as a tool to target the victim for the execution of the desired crime. Though it is difficult to determine that where the particular cyber crime took place because it can harm its victim even sitting at a far distance. As stated above from the year 1997 to 2008 tremendous changes took place which helps the judicial system to determine the specific kind of cyber crime. However, all cybercrimes involved both the computer and the person behind it as victims, it just depends on which of the two is the main target.

Example: 1 – Hacking involves attacking the computer's information and other resources;

Example: 2 – Stalking involves attacking the personal space of an individual.

Cyber crimes are quite different from traditional crimes as they are often harder to detect, investigate and prosecute and because of that cyber crimes cause greater damage to society than traditional crimes. Cyber crime also includes traditional crimes conducted through the internet or any other computer technology. For example; defamation, forgery, identity theft, terrorism, cyber-stalking, hacking, software piracy,

[4] What Is Digital Risk? Table of Contents. Types of Digital Risk. Digital Risk Protection. How to Manage Digital Risk. How Proofpoint Can Help. https://www.proofpoint.com/

web jacking and bullying are considered to be cyber crimes when traditional crimes are committed through the use of a computer and the internet.

However, the cyber crimes are broadly classified into different groups:

1 Crime against the individuals – Harassment, cyber-stalking, deformation, indecent exposure, cheating, email spoofing, fraud, etc;

2 Crime against property – Transmitting virus, net-trespass, unauthorized control over computer system, internet thefts, infringement of intellectual property, etc;

3 Crime against organization – Cyber terrorism within government organization, possession of unauthorized information, distribution of pirate software, etc;

4 Crime against society – Child pornography, financial crimes, sale of unlawful articles, trafficking, forgery of records, gambling, etc[5].

According to the World Economic Forum (WEF), cybercrime has emerged as the world's third-largest economy, trailing only the United States and China.

Cybersecurity Ventures, projects that its impact will reach $10.5 trillion by 2025… The availability of online access to networks and ransomware has played a pivotal role in driving this exponential growth, and this accessibility has opened the doors for individuals with varying levels of technical expertise to launch sophisticated cyber and ransomware attacks[6].

Through the pointers below, our views on this threat may change completely:

Not only scientists have touched on this danger, but also the following organization comopany:

Cybercrime is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic, and international response.

[5] Cyber Laws. Cyber crime. Unit 5. 5.2 Cyber crime and its classification. https://egyankosh.ac.in/bitstream/123456789/73775/1/Unit-5.pdf:

[6] CYBERCRIME IS WORLD'S THIRD-LARGEST ECONOMY. https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy/#:~:text=our%20interconnected%20world.-,According%20to%20the%20World%20Economic%20Forum%20(WEF)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6

UNODC promotes long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action. Specifically, UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness-raising, international cooperation, and data collection, research, and analysis on cybercrime[7].

Taking everything into account, the article underscores the indispensable role of digital technology in our contemporary world, presenting a dual landscape of advantages and threats. Digital risk, as defined by experts like Saptarshi Ganguly and others, encompasses the consequences of digital enablements that enhance risk effectiveness. The narrative explores the heightened concern of digital risk, especially for displaced populations, highlighting unique barriers they face in accessing digital services. It introduces a Learning Lab session to categorize and assess digital risks, offering a framework to support organizations and UN agencies. The article delves into the complexity of digital risks, categorizing them into nine primary types. It emphasizes the need for proactive digital risk protection strategies, outlining various methodologies. The discussion extends to cybercrime, detailing its classification and the alarming projection of its economic impact. In a world increasingly interconnected, managing digital risks becomes paramount for organizations and societies alike.

References:

1. **Digital risk: Transforming risk management for the 2020s.** February 10, 2017 | Article. **By Saptarshi Ganguly, Holger Harreis, Ben Margolis, and Kayvaun Rowshankish. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/digital-risk-transforming-risk-management-for-the-2020s;**
2. What is Digital Risk? Definition and Protection Tactics for 2023. Cybersecurity Writer Edward Kost. https://www.upguard.com/blog/digital-risk#:~:text=Digital%20risk%20refers%20to%20all,its%20exposure%20to%20cyber%20threats;
3. Internet Security Alliance. https://chapters.acp-international.com/images/newyorkcitymetro/ACO_NY_Metro-7-19-17.pdf;
4. What Is Digital Risk? Table of Contents. Types of Digital Risk. Digital Risk Protection. How to Manage Digital Risk. How Proofpoint Can Help. https://www.proofpoint.com/;
5. Cyber Laws. Cyber crime. Unit 5. 5.2 Cyber crime and its classification. https://egyankosh.ac.in/bitstream/123456789/73775/1/Unit-5.pdf:
6. CYBERCRIME IS WORLD'S THIRD-LARGEST ECONOMY. https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy/#:~:text=our%20interconnected%20world.-,According%20to%20the%20World%20Economic%20Forum%20(WEF)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6;
7. Cybercrime. Unatied Nations. UNODC Romena. Cybercrime. https://www.unodc.org/romena/en/cybercrime.html.

[7] Cybercrime. Unatied Nations. UNODC Romena. Cybercrime. https://www.unodc.org/romena/en/cybercrime.html.